IBM Security Guardium V10.1

Tabla de contenido

Bienvenido 1

Visión general del producto 1
IBM Guardium 1
Novedades de este release 2
Notas del release 5

Guía de inicio 6
Guía de inicio a la interfaz de usuario 6
Personalización de la interfaz de usuario 8
Inicio rápido para la supervisión y cumplimiento 8
Vista de sistema 9
Supervisión de actividad de datos 9
Políticas y reglas 10
Flujos de trabajo 10
Auditoría 10
Clasificación 10
Supervisión de actividad de archivos 10
Visión general y conceptos para la supervisión de actividad de archivos (FAM) 11
Requisitos previos para la supervisión de actividad de archivos 12
Flujo de trabajo de nivel superior para la supervisión de actividad de archivos 13
Conceptos clave y herramientas 13
Consulta e informes 13
Control de acceso 13
Roles de usuario 14
Grupos 14
Depuración y archivado de datos 14
Guardium Installation Manager 14

Descubrir 15
Orígenes de datos 15
Creación de una definición de origen de datos 15
Cómo trabajar con orígenes de datos existentes 20
Informes sobre orígenes de datos 21
Definición de un origen de datos utilizando un nombre de servicio 21
Gestión de definiciones de KDC 21
Protección del servicio de base de datos en la nube 22
Flujo de trabajo de protección del servicio de base de datos en la nube 23
Definición de IAM de AWS 23
Crear, modificar, suprimir cuentas en la nube 24
Descubrir bases de datos en la nube 25
Catalogar y gestionar bases de datos 25
Gestionar el asesoramiento de vulnerabilidades y la clasificación 26
Configurar la auditoría de bases de datos 26
Modificar el límite de objetos añadidos automáticamente y el recopilador
Habilitar la auditoría en una base de datos
Inhabilitar la auditoría en una base de datos
Poseer o dejar de poseer la auditoría de bases de datos
Gestionar auditoría de objetos 28
Gestión de auditoría de objetos en una base de datos 29
Gestión de auditoría de objetos en varias bases de datos 29
Descubrimiento automático de base de datos 30
Clasificación 31
Rendimiento del proceso de clasificación 32
Gestión de reglas de clasificación 32
Cómo trabajar con procesos de clasificación 33
Cómo trabajar con políticas de clasificación 34
Cómo trabajar con reglas de clasificación 34
Cómo trabajar con acciones de regla de clasificación 36
Descubrir datos confidenciales 37
Escenario de descubrimiento 38
Nombre y descripción 38
Qué se va a descubrir 39
Criterio de regla 40
Contenido de miembro real 41
Área de búsqueda 41
Ejecutar descubrimiento y revisar informe 42

Auditoría 42
Planificación 43
Expresiones regulares 43
Descubrir y clasificar datos confidenciales en servidores de archivos 46
Instalación y activación de los componentes de supervisión de actividad de archivos 46
Parámetros GIM de descubrimiento y clasificación de archivos 47
Personalización de planes de decisiones de FAM 49
Optimización de titularidades 51
Habilitar y configurar la optimización de titularidades 51
Novedades de la optimización de titularidades 53
Usuarios y roles de optimización de titularidades 53
Recomendaciones de optimización de titularidades 53
Examinar las titularidades de la optimización de titularidades 54
Probabilidad de optimización de titularidades 55

Protección 55
Líneas base 56
Políticas 59
Pruebas de patrones especiales 61
Acciones de regla 62
Creación de políticas 67
Instalación de políticas 71
Campos de definición de regla 74
Integración de reglas personalizadas con políticas de Guardium 78
Utilización de la acción Ignorar adecuada 84
Conjuntos de caracteres 85
Alertas de correlación 103
Señalización de sucesos a través de las alertas de correlación 104
Gestión de incidencias 107
Gestión de la revisión de las incidencias de seguridad de varias bases de datos 108
Reescritura de consultas 111
Cómo funciona la reescritura de consultas 111
Utilización de la reescritura de consultas 112
Habilitación de la reescritura de consultas 112
Creación de definiciones de reescritura de consultas 113
Cómo probar las definiciones de reescritura de consulta 113
Definición de una política de seguridad para activar la reescritura de consultas 114
Creación de un informe personalizado para validar los resultados de la reescritura de consultas 115
Reglas y políticas de la actividad de archivos 116
Funcionalidad de reglas y políticas de actividad de archivos 116
Creación de una nueva política de FAM y de sus reglas 118
Creación de una regla de política de FAM desde el separador de titularidades del Panel de control de investigación 119

Supervisar y auditar 119
Creación de procesos de auditoría 120
Cómo crear un flujo de trabajo de auditoría 129
Abrir los resultados de proceso de flujo de trabajo 132
Cómo distribuir el flujo de trabajo a través de grupos de Guardium 132
Lista de tareas pendientes de proceso de auditoría 141
Auditoría e informes 141
Correlación de datos externos 142
Conjuntos de privacidad 147
Alertas personalizadas 148
Proceso Flat Log 150
Crear expresión en condición de consulta 150
Informes de titularidad de base de datos 151
Identificación de usuario 151
Identificar usuarios a través de la conversión de usuarios de aplicación 152
Identificar usuarios mediante API 156
Identificar usuarios a través de procedimientos almacenados 159
Auditoría de cambio de valores 160
Crear una base de datos de auditoría 161
Acceso a tablas supervisadas 163
Inicio rápido para la supervisión del cumplimiento 164
Requisitos previos para la supervisión de cumplimiento 165
Configurar supervisión del cumplimiento 167
Rellenar grupos 168
Habilitar el escaneo de datos confidenciales 168
Interpretación de las vistas de supervisión de cumplimiento 169
Cómo utilizar PCI/DSS Accelerator para implementar el cumplimiento de PCI 170
Creador de flujos de trabajo 174

Cómo crear flujos de trabajo personalizados 175
Cómo utilizar los flujos de trabajo personalizados 176
Análisis de detección de amenazas 178
Características de un ataque de inyección de SQL 178
Características de un ataque de procedimientos almacenados 178
Habilitación de análisis de detección de amenazas 178
Cómo trabajar con informes de casos 179
Activación del flujo de trabajo del proceso de auditoría para el análisis de amenazas 179
Cómo trabajar con paneles de control de diagnóstico de amenazas 180
Investigación de amenazas de inyección de SQL 180
Investigación de amenazas de procedimientos almacenados 181
Funciones de análisis de detección de amenazas 182
Paneles de control de investigación 186
Habilitación e inhabilitación del panel de control de investigación 187
Habilitación de actividad de archivos en el panel de control de investigación 188
Acceso al panel de control de investigación 188
Panel de control de investigación para datos 189
Panel de control de investigación para archivos 189
Filtrado de datos y guardado de filtros en el panel de control de investigación 190
Filtrado de un gráfico individual 191
Creación, guardado y exportación de paneles de control de investigación 191
Utilización de la vista de topología 192
Búsqueda local y distribuida 193
Utilización de visión de datos 193
Detección de valores atípicos 194
Inicio rápido para la detección de valores atípicos 195
Habilitación e inhabilitación de la detección de valores atípicos en un agregador 196
Habilitación e inhabilitación de la detección de valores atípicos localmente en un recopilador 196
Interpretación de valores atípicos de datos en el panel de control de investigación 197
Interpretación de los valores atípicos de actividad de archivos 199
Supervisar el estado de minería de valores atípicos 199
Agrupación de usuarios y objetos para la detección de valores atípicos 200
Exclusión de sucesos de la detección de valores atípicos 201
Panel de control de protección de datos 202

Informes 203
Parámetros de informe 206
Creación de paneles de instrumentos 206
Visualización de un informe 207
Renovación de informes 208
Exportación de un informe 209
Visualización de informes profundizables 209
Creación de un informe 209
Creación de informes para z/OS 210
Despensa de datos 210
Auditoría e informes 219
Consultas 219
Utilización del Creador de consultas 220
Condiciones de consulta 222
Dominios, entidades y atributos 224
Dominios 225
Dominios personalizados 227
Entidades y atributos 234
Informes de titularidad de base de datos 268
Cómo sacar provecho de los informes predefinidos 277
Informes predefinidos 280
Informes de administrador predefinidos 281
Informes de usuario predefinidos 300
Común de informes predefinidos 307
Cómo formular preguntas de los datos 308
Cómo informar sobre columnas y tablas latentes 311
Cómo generar la Llamada de API desde Informes 314
Cómo utilizar Constantes en Llamadas de API 318
Cómo utilizar llamadas de API desde informes personalizados 322
Canal de información externo opcional 327
Correlación de un canal de información externo 327
Creador de informes distribuidos 328
Cómo crear un Informe distribuido 332

Asesorar y reforzar 334
Inicio al asesoramiento de vulnerabilidades de Guardium 335

Privilegios de base de datos para clasificación y asesoramiento de vulnerabilidades 338
Despliegue de asesoramiento de vulnerabilidades para DB2 para i 339
Utilización del asesoramiento de vulnerabilidades con Cloudera 340
Pruebas de asesoramiento de vulnerabilidades 343
Definición de una prueba basada en consultas 344
Definición de pruebas basadas en CAS 346
Asesoramientos 346
Creación de un asesoramiento 346
Creación de una excepción de prueba de VA 347
Cómo crear un asesoramiento de seguridad 347
Ejecución de un asesoramiento 352
Visualización de resultados de asesoramiento 352
Resumen del asesoramiento de vulnerabilidades 354
Cambio de esquema necesario 354
Asesoramiento de vulnerabilidades de RACF 355
CAS (Configuration Auditing System) 355
Sustitución por anomalía e inicio de Configuration Auditing System (CAS) 358
Plantillas de CAS 360
Cómo trabajar con plantillas de CAS 365
Hosts de CAS 367
Creación de informes de CAS 369
Estado de CAS (Configuration Auditing System) 375

Configuración del sistema Guardium 376
Configuración del sistema 376
Configuración del motor de inspección 378
Configuración de portal 381
Generar nuevo diseño 382
Configurar la autenticación 382
Perfil global 383
Configuración del alertador 387
Detección de anomalías 388
Inferencia de sesiones 389
Creación de alias IP-Nombre de host 389
Copia de seguridad del sistema 390
Configuración de la copia de seguridad de parche 393
Configurar permiso para la conexión de socket 393

Visión general de la gestión de acceso 394
Roles 395
Gestión de roles y permisos 397
Cómo crear un rol con acceso mínimo 398
Gestionar usuarios 398
Cómo crear un usuario con las titularidades correctas para iniciar sesión en la CLI 401
Importación de usuarios de LDAP 402
Seguridad de datos - Jerarquía de usuarios y asociaciones de base de datos 404
Cómo definir jerarquías de usuario 405
Inicio de sesión en la interfaz de usuario de Guardium mediante una tarjeta inteligente 407

Agregación y gestión central 409
Agregación 409
Gestión central 415
Servicios de componentes de Guardium 416
Implementación de la gestión central 418
Implementación de la gestión central en una instalación nueva 418
Registro de unidades 419
Desregistro de una unidad gestionada 420
Sincronización de cuentas de usuario del portal 420
Implementación de la Gestión central en una instalación existente 421
Utilización de las funciones de Gestión central 422
Vistas de salud de despliegue 422
Configuración de un gestor central para las vistas de salud de despliegue 423
Vistas de tabla y topología de salud de despliegue 423
Panel de control de salud de despliegue 425
Escenario: Resolución de problemas de sistemas sobrecargados mediante la vista de topología de salud de despliegue 428
Inventario de despliegue 428
Vista Despliegue de recursos 428
Creación de grupos de unidades gestionadas 428
Supervisión de unidades gestionadas 429
Instalación de políticas de seguridad en unidades gestionadas 432
Gestión central de parches 432

Utilización de perfiles de configuración 433
Distribuir configuración 434
Distribuir configuración de autenticación 434
Redundancia de la Gestión central 434
Centro de investigación 437

Gestión del sistema Guardium 439

Administración de Guardium 440
Certificados 441
Nivel de utilización de unidad 443
Configuración del proceso de datos de utilización de unidad 444
Subidas de cliente 445
Panel Estado de Servicios 448
Archivado, depuración y restauración 448
Catálogo de Guardium 454
Cómo gestionar la copia de seguridad y el archivado 454
Exportación de resultados (CSV, CEF, PDF) 457
Exportar/Importar definiciones 457
Interfaz distribuida 460
Gestionar clases personalizadas 461
Subida de un archivo de claves 461
Claves públicas SSH 462
Cómo instalar un certificado de dispositivo para evitar un reto de certificado SSL del navegador 462
Autosupervisión 464
Cómo supervisar el sistema Guardium mediante alertas 466
Supervisión con SNMP 469
Supervisor de consultas en ejecución 471
Grupos 471
Visión general de grupos 471
Utilización del creador de grupos 472
Creación y edición de grupos 472
Visualización de la pertenencia a grupos y su utilización 473
Cumplimentación de grupos 473
Importación desde orígenes de datos externos 474
Utilización del creador de grupos (antiguo) 474
Creación de un nuevo grupo 475
Modificación de un grupo 475
Cumplimentación de grupos 476
Cómo llenar un grupo desde LDAP 476
Llenado de un grupo a partir de una consulta 477
Llenado de un grupo a partir de procedimientos almacenados 478
Llenado de un grupo utilizando orígenes de base de datos 479
Llenado de un grupo utilizando dependencias de base de datos 479
Llenado de un grupo utilizando dependencias inversas 480
Llenado de un grupo utilizando procedimientos observados 480
Llenado de un grupo utilizando Generar objeto seleccionado 480
Utilización de grupos en consultas y políticas 481
Ejemplo: Utilización de grupos para crear reglas y políticas 481
Grupos predefinidos 482
Roles de seguridad 486
Notificaciones 487
Cómo crear una alerta en tiempo real 487
Administración de clase de alerta personalizada 488
Alertas predefinidas 489
Planificación 490
Alias 490
Fechas e indicaciones de fecha y hora 491
Periodos de tiempo 493
Periodos de tiempo 493
Comentarios 494
Cómo instalar parches 494
Mantenimiento de soporte 496

Integración de productos 496

Configurar BIG-IP Application Security Manager (ASM) para la comunicación con el sistema Guardium 496
Integración de Hadoop 497
Integración de Hadoop utilizando un S-TAP estándar de Guardium 497
Recomendaciones y limitaciones 498
S-TAP y motores de inspección con Hadoop 498
Políticas y reglas de Guardium con Hadoop 499
Informes de Guardium con Hadoop 499

Integración de Hadoop utilizando Cloudera Navigator 500
Planificación de la integración con Cloudera Navigator 501
Configurar la solución para la supervisión 501
Configurar la comunicación entre Guardium y Cloudera Navigator 502
Integración de Hadoop utilizando Hortonworks y Apache Ranger 502
Planificación de la integración con Hortonworks y Apache Ranger 503
Configurar la solución para la supervisión 504
Configurar la comunicación entre Guardium y Ranger 504
Instalar y configurar los S-TAP 504
Habilitar la supervisión para los servicios Hadoop 505
Integración de PIM 505
Integración de QRadar y Guardium 507
Interfaz de OPTIM a Guardium 508
Combinación de alertas en tiempo real y análisis de correlación con productos SIEM 508
Cómo transferir datos confidenciales a InfoSphere Discovery 511
Correlación con CEF 513
Correlación LEEF 515

Resolución de problemas 516
Técnicas de resolución de problemas 517
Obtención de arreglos de Fix Central 518
Cómo ponerse en contacto con el soporte de IBM 518
Información básica del soporte de IBM 519
Intercambio de información con IBM 521
Suscripción a actualizaciones de soporte 522
Problemas y soluciones 523
Interfaz de usuario 523
Los cambios no se guardan cuando se añade un motor de inspección 523
Error HTTP 403 524
Java.lang.IllegalStateException 524
Las páginas no se están cargando correctamente 524
Políticas 525
La consulta no aparece en la definición de alerta de correlación 525
La regla no se desencadena 525
La función Redactar causa un resultado excesivamente enmascarado 526
Las sesiones SSH y los trabajos CRON automatizados que inician sesión en la base de datos de Oracle se muestran como inicios de sesión fallidos. 526
La base de datos interna de Guardium se está llenando 527
Informes 527
No puede modificar la tabla de receptor para un proceso de auditoría después de que se haya ejecutado al menos una vez 527
No se pueden ver caracteres de varios bytes 528
El sistema de archivos está casi lleno 528
Los informes de auditoría de Guardium visualizados en Microsoft Excel tienen filas con caracteres inesperados 529
Los informes muestran la dirección IP como 0.0.0.0 529
Mensaje La solicitud se ha interrumpido o se ha excedido la cuota 529
La regla no se desencadena 525
Excepciones de trabajos planificados cada 5 minutos 530
Excepción de trabajos planificados: Se requiere fusión, retardo al ejecutar proceso 531
El usuario de la base de datos no se muestra correctamente en los informes de Guardium cuando se supervisa Teradata 531
Resultados inesperados en informes de Guardium con mandatos incluidos 531
Evaluar y reforzar 532
CAS no funciona con Java 1.7 en Windows 532
Miembros del grupo de excepciones Asesoramiento de vulnerabilidades aparecen en la prueba fallida 532
Configuración del sistema Guardium 533
No se puede configurar STAP después de la actualización 533
Guardium no puede reconocer el dispositivo de red VMXNET x 533
Error de interfaz de red de Guardium después de sustituir la placa del sistema 534
La máquina virtual Guardium no es accesible desde la red 534
SSLv3 está habilitado 535
Gestión de acceso 535
No se puede iniciar sesión en Guardium, salvo como admin o accessmgr 536
Restablecimiento de la contraseña de accessmgr de Guardium 536
Agregación 536
No se puede convertir el recopilador de Guardium en agregador 536
Un cambio de configuración de Exportación de datos desde la interfaz gráfica de usuario de un sistema gestionado Guardium falla con error 537
Diferencias entre resultados y el informe del proceso de auditoría 537
Errores HY000 después de restaurar la configuración en un agregador 538
Gestión central 538
Un usuario está inhabilitado en una unidad gestionada de Guardium, pero se muestra como habilitado en el Gestor central 539
El Gestor central no reconoce la nueva versión de las unidades actualizadas 539
Las tareas planificadas no se activan a la hora planificada 539
Excepción de Torque en la vista Gestión central de la interfaz gráfica de usuario 540

S-TAP y otros agentes 540
Error de AIX 6.1 al instalar o actualizar el S-TAP dex IBM Security Guardium 540
Error al abrir el área de memoria compartida cuando se configura COMM_EXIT_LIST de Guardium para DB2 541
Guardium no puede recopilar el tráfico de la memoria compartida de Informix 542
Uso elevado de CPU y E/S en el host STAP de Guardium 542
Falta información del paquete de inicio de sesión 543
El proceso nanny interrumpe sniffer 543
Sniffer no se puede conectar a UNIX S-TAP 543
S-TAP no se puede iniciar 544
S-TAP no se inicia automáticamente en Linux 544
S-TAP devuelve "Not FIPS 140-2 complaint" 544
El módulo de kernel K-TAP sigue presente tras la desinstalación de S-TAP 545
S-TAP de UNIX no puede leer más de 16 motores de inspección 545
El servicio S-TAP de Windows se cuelga al iniciarse con el ID de error 1000 546
S-TAP de z/OS no se muestra activo en el sistema Guardium 546
GIM 547
Error al instalar Guardium Installation Manager (GIM) 547
El servicio Guardium Installation Manager (GIM) no se inicia en Windows 547
Actividad de archivos 547
La actividad de archivos no se registra en los informes o panel de control de investigación 548
La actividad de archivos del disco extraíble no se registra en el panel de control de investigación 548
La actividad de archivos aparece en los informes pero no en el panel de control de investigación 548
Faltan algunos archivos de los resultados de clasificación 548
Resultados de descubrimiento parcial de archivos (titularidad) en informes y en el panel de control de investigación 548
Faltan resultados de clasificación de archivos en los informes y el panel de control de investigación 549
El paquete de FAM no se puede instalar 549
Instalación del sistema Guardium 549
Error de suma de comprobación durante la instalación de S-TAP 550
S-TAP de Guardium devuelve un mensaje de error de cp: opción -f no permitida 550
La instalación de un nuevo parche de Guardium no se completa 550
Falta un archivo o directorio después de una instalación nueva de S-TAP de Guardium 551
Error de partición al instalar Guardium 551
Falla la instalación de parche: no existe ese archivo o directorio 552

S-TAPs y otros agentes 552
Instalación de S-TAP 553
Instalación de un S-TAP en un servidor Windows 555
Instalación de S-TAP de Windows mediante Guardium Installation Manager 556
Instalación de S-TAP de Windows mediante el instalador interactivo 557
Instalación de Windows S-TAP mediante la interfaz de línea de mandatos 558
Referencia de la instalación desde la línea de mandatos de S-TAP de Windows 558
Actualización y eliminación de un S-TAP en Windows 559
Instale el cliente de S-TAP en un servidor Linux, Solaris, AIX o HP-UX 560
Elección de la configuración de S-TAP 561
Instalación del cliente S-TAP en servidores Linux, Solaris, AIX y HP-UX con GIM 563
Instalación y desinstalación de S-TAP en un servidor Linux, Solaris, AIX y HP-UX utilizando RPM 564
Instalación de STAP de Linux, Solaris, AIX y HP-UX utilizando el instalador de shell 566
Parámetros de script de instalación de STAP para UNIX 567
Instalación y desinstalación de un S-TAP de Linux, Solaris, AIX y HP-UX con un instalador nativo 567
Instalación y desinstalación de S-TAP con el instalador nativo de AIX 568
Instalación y desinstalación de S-TAP con un instalador nativo HP-UX 568
Instalación y desinstalación de S-TAP con el instalador nativo de Solaris 569
Desinstalación de S-TAP 569
Trabajar con K-TAP 569
El mecanismo de los K-TAP 570
Creación de un K-TAP en Linux 571
Copia de un nuevo módulo K-TAP en otros sistemas 571
Obtención de información de Java o Perl 571
Cuándo reiniciar o rearrancar la base de datos después de la instalación o actualización de S-TAP 572
Equilibrio de carga empresarial 574
Utilización del equilibrio de carga empresarial 575
Configuración de instalaciones de S-TAP para el equilibrio de carga empresarial 575
Asociación de S-TAP con unidades gestionadas para el equilibrio de carga 576
Visualización del mapa de carga de equilibrio de carga empresarial 576
Visualización de un informe de actividad de equilibrio de carga empresarial 577
Parámetros de configuración del equilibrio de carga empresarial 577
Tráfico de base de datos autenticado mediante Kerberos 579
Autenticación Kerberos: bases de datos soportadas 579
Habilitación del plugin de Kerberos 580
Configuración del plugin de Kerberos 580
Búsqueda de los parámetros de configuración de Kerberos para Oracle 581

Búsqueda de los parámetros de configuración de Kerberos para Sybase 581
Utilización de bibliotecas de salida 581
Integración de DB2 Exit con S-TAP 581
Integración de Informix Exit con S-TAP de UNIX 584
Integración de Teradata Exit con STAP de UNIX 585
Configuración especial de entornos Linux, Solaris, HP-UX y AIX 586
Configuración de STAP para zonas de Solaris 586
Configuración de S-TAP de Oracle RAC 586
Configuración de S-TAP para WPAR de DB2 587
Activación de A-TAP en todos los nodos de un clúster de DB2 588
Configuración del montaje retardado en disco de clúster 589
Guía de administración de S-TAP 589
Configuración del sistema Guardium para gestionar S-TAP 591
Certificación de S-TAP 592
Configuración de la autenticación de S-TAP con certificados SSL 592
Aumento del rendimiento de S-TAP 598
S-TAP de UNIX 598
S-TAP de Windows 609
S-TAP Discovery 612
Gestión de A-TAP 612
Preparación para la configuración y el mantenimiento de A-TAP 613
Configuración y activación de A-TAP 613
Directrices para la activación y desactivación de A-TAP y para la detención y reinicio de la BD 614
Mandatos del programa de utilidad guardctl para A-TAP 614
Códigos de retorno de guardctl 616
Parámetros de guardctl específicos de la base de datos 617
Parámetros de guardctl específicos de Oracle 617
Parámetros de guardctl específicos de Sybase 618
Parámetros de guardctl específicos de DB2 (solo Linux) 618
Parámetros de guardctl específicos de Informix 619
Parámetros de guardctl específicos de Postgres 619
Desactivación de A-TAP 620
Configuración y activación de A-TAP en entornos especiales 620
Instalación y activación de A-TAP en entornos de zonas y WPAR 620
Desactivación y desinstalación de A-TAP en entornos de zonas y de WPAR 621
Actualización de ATAP en entornos de zonas y WPAR 622
Pasos para configurar y activar A-TAP para una base de datos Teradata 622
Configuración de Oracle para A-TAP 624
Resolución de problemas de configuración de A-TAP 624
Tee 625
Configuración de S-TAP desde la GUI 629
Edición de los parámetros de configuración de S-TAP 638
Parámetros de S-TAP de Windows 638
Parámetros de SQLGuard 638
Parámetros generales 639
Parámetros del motor de inspección 641
Parámetros de cortafuegos 642
Parámetros del servidor de aplicaciones 643
Parámetros de depuración 643
Parámetros de CAS (Configuration Auditing System) 644
Parámetros del controlador 645
Parámetros de S-TAP de UNIX 645
Parámetros de SQLGuard 646
Parámetros generales 647
Parámetros de Hadoop 650
Parámetros del motor de inspección 652
Parámetros de cortafuegos 654
Parámetros del servidor de aplicaciones 654
Parámetros de descubrimiento 655
Parámetros de CAS (Configuration Auditing System) 655
Parámetros de depuración 655
Parámetros de K-TAP 656
Configuración del montaje retardado en disco de clúster 589
Supervisor de estado de S-TAP 658
Visualización de los resultados de la verificación de S-TAP 658
Configuración de la planificación de verificación de S-TAP 659
Resolución de problemas de S-TAP en la plataforma Linux 659
Supervisión del comportamiento de S-TAP 660
Panel de sucesos de S-TAP 667
Informes de S-TAP 667
Mensajes de error de S-TAP 668
Apéndice de S-TAP 668

Instalación, inicio y detención de CAS desde la línea de mandatos 668
Definiciones de IMS 669
DB2 for i S-TAP 669
Estrategia de supervisión 670
Instalación del S-TAP para IBM i 671
Definición del S-TAP para IBM i 672
IBM Security Guardium S-TAP for z/OS 673

Guardium Installation Manager 675

Inicio rápido para desplegar agentes de supervisión 676
Requisitos previos para desplegar agentes de supervisión 676
Desplegar agentes de supervisión 676
Gestión de software con GIM 677
Configuración por cliente 677
Interfaces de usuario de GIM 678
Interfaz de línea de mandatos de GIM 681
Asignación de servidores GIM 684
Instalación del cliente GIM en un servidor Windows 686
Instalación del cliente GIM en un servidor UNIX 688
Actualización del cliente GIM 688
Utilización de grupos con GIM 688
Cómo copiar un módulo K-TAP mediante GIM 689
Actualización dinámica de GIM 689
Cuando actualice el sistema operativo del servidor de base de datos 690
Distribución de lotes de GIM a unidades gestionadas 690
Eliminación de lotes de GIM no utilizados 691
Ejecución de diagnósticos de GIM 691
Depuración de operaciones de GIM 692
Reinicio del supervisor para Solaris con soporte de SMF 692

Instalación del sistema Guardium 692

Modalidades operativas 693
Claves de licencia 693
Requisitos de hardware 694
Requisitos de los puertos de Guardium 694
Paso 1. Ensamblar lo siguiente antes de comenzar 697
Dispositivos de almacenamiento SAN 698
Paso 2. Configurar el dispositivo físico o virtual 698
Dispositivo físico 698
Cómo identificar eth0 y otros puertos de red 698
Contraseñas predeterminadas para dispositivos físicos 699
Dispositivo virtual 699
Paso 3. Instalar la imagen de Guardium 699
Paso 4. Establecer la configuración inicial y básica 700
Establecer la dirección IP del sistema primario 700
Establecer la dirección IP predeterminada del direccionador 700
Establecer la dirección IP del servidor DNS 700
Servidor SMTP 701
Establecer el nombre de host y el nombre de dominio 701
Establecer el huso horario, la fecha y la hora 701
Establecer el tipo de unidad inicial 701
Restablecer la contraseña root 701
Validar todos los valores 702
Rearrancar el sistema 702
Paso 5. Qué hacer a continuación 702
Verificar si la instalación es correcta 703
Establecer el tipo de unidad 703
Instalación de las claves de licencia 703
Instalar parches de mantenimiento (si están disponibles) 704
Pasos adicionales (opcional) 704
Crear la imagen virtual 705
Visión general de la infraestructura de VMware 705
Visión general de la instalación de la MV 705
Creación de una máquina virtual de Hyper-V 708
Particionamiento personalizado 709
Cómo realizar una partición con un LVM cifrado 709
Ejemplo de configuración de SAN 710

Actualización del sistema Guardium 712

Planificación de una actualización 713
Elección de un método de actualización 713

Entornos de versiones mixtas durante una actualización 714
Actualización con gestores centrales y agregadores 715
Tareas de actualización comunes 715
Depurar datos del sistema 715
Instalación, distribución y supervisión de parches 716
Seguimiento del progreso de la instalación con diag 716
Verificación y limpieza después de la actualización 717
Actualizar un entorno de 32 bits 717
Actualizar un gestor central de 32 bits 717
Actualizar unidades gestionadas de 32 bits 718
Actualizar un entorno de 64 bits 719
Actualizar un gestor central de 64 bits 719
Actualizar unidades gestionadas de 64 bits 720
Actualizar un entorno de 32 bits sin un gestor central de copia de seguridad 721
Actualizar un gestor central de copia de seguridad de 32 bits 721
Actualizar el gestor central primario de 32 bits antiguo 723
Actualizar unidades gestionadas de 32 bits 723
Actualizar un entorno de 64 bits con un gestor central de copia de seguridad 724
Actualizar un gestor central de copia de seguridad de 64 bits 725
Actualizar el gestor central primario de 64 bits antiguo 726
Actualizar unidades gestionadas de 64 bits 727

CLI y API 728
Visión general de CLI 728
Mandatos de CLI del agregador 730
Mandatos de CLI del alertador 733
Mandatos de CLI de certificados 735
Mandatos de CLI de configuración y control 739
Mandato de CLI diag 760
Mandatos de CLI de manejo de archivos 769
Mandatos de CLI del motor de inspección 776
Mandatos de CLI del panel de control de investigación 779
Mandatos de CLI de configuración de red 779
Mandatos de CLI de soporte 784
Mandatos de CLI sistema 791
Mandatos de CLI de cuenta de usuario, contraseña y autenticación 797
Referencia de GuardAPI 803
Funciones de archivado y restauración de GuardAPI 807
Funciones de asesoramiento de GuardAPI 809
Funciones de descubrimiento automático de GuardAPI 813
Funciones de entrada de catálogo de GuardAPI 816
Funciones de clasificación de GuardAPI 818
Funciones de orígenes de datos de GuardAPI Cloud 830
Funciones de usuario de base de datos de GuardAPI 832
Funciones de orígenes de datos de GuardAPI 834
Funciones de referencia de orígenes de datos de GuardAPI 840
Funciones de seguridad de usuario de datos de GuardAPI 842
Funciones de equilibrio de carga de empresa de GuardAPI 846
Funciones de optimización de titularidades de GuardAPI 847
Funciones de canal de información externo de GuardAPI 848
Funciones de FAM (File Activity Monitor) de GuardAPI 849
Funciones GIM de GuardAPI 851
Funciones de grupo de GuardAPI 860
Generación de entrada de GuardAPI 867
Funciones del panel de control de investigación de GuardAPI 875
Funciones de auditoría nativas de GuardAPI 876
Funciones de detección de valores atípicos de GuardAPI 879
Funciones de control de procesos de GuardAPI 879
Funciones de reescritura de consultas de GuardAPI 893
Funciones de rol de GuardAPI 907
Funciones de GuardAPI S-TAP 911
Funciones de detección de amenazas de GuardAPI 182

S-TAP for z/OS V10.1.3 User's Guide 923
IBM Security Guardium S-TAP for Db2 on z/OS 923
IBM Security Guardium S-TAP for Db2 on z/OS overview 924
What's new in IBM Security Guardium S-TAP for Db2 on z/OS V10.1.3? 924
The IBM Security Guardium S-TAP for Db2 on z/OS installation environment 924
Installation and operation requirements 925
Compatibility with IBM Db2 Query Monitor for z/OS and other products 926
Required user ID authorizations 926

Configuring IBM Security Guardium S-TAP for Db2 on z/OS 927
Upgrading from previous versions of InfoSphere Guardium S-TAP for DB2 927
Configuring IBM Security Guardium S-TAP for Db2 on z/OS 927
APF authorizing the LOAD library data set 928
Enabling the dynamic LPA facility service CSVDYLPA 928
Service class considerations 928
Customizing JCL members 929
Creating the IBM Guardium S-TAP for Db2 control file 929
Configuring the IBM Guardium S-TAP for Db2 control file 929
Required statements for each subsystem 929
Configuring the collector agent 930
Configuring the JCL for ADHBIND 930
Configuring the JCL for ADHGRANT 930
Configuring the ADHCFGP data set 930
Defining the collector agent started task JCL 931
Configuring the collector agent for additional Db2 subsystems 932
Support Services Address Space overview 932
Usage considerations for the Master Address Space 932
Stopping the Master Address Space 933
Enabling CICS Login User ID reporting 933
Data collection 933
Data collection process 934
Collection policy 934
Collected event types 934
Audit data for Db2 Utilities 935
Filtering 935
Event types and filtering 936
Filtering by database name 937
Filter wildcard support 937
Policy pushdown 937
Streaming audit data to multiple systems 938
Starting and stopping the collector agent 938
Including or excluding failed accesses and negative SQL code 938
Quarantining SQL activity 939
SQL Blocking 939
Controlling host variable collection 939
Collecting Command activity by using the Audit SQL Collector 940
Collecting SET CURRENT SQLID events by using the Audit SQL Collector 940
Reference information 940
Sample library members 940
MODIFY command 941
S-TAP logging 943
Collector agent parameters 943
Keeping connections active when HOT_FAILOVER is enabled 952
Collector agent sample parameter file 952
ADHEMAC1 edit macro variables 953
Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS 954
Error messages 954
Error messages and codes: ADHAxxx 954
ADHA507E 954
Error messages and codes: ADHGxxx 955
ADHG000I 956
ADHG001I 956
ADHG002I 956
ADHG003I 956
ADHG004W 957
ADHG005S 957
ADHG006E 957
ADHG007E 957
ADHG008S 957
ADHG009I 957
ADHG010I 958
ADHG011E 958
ADHG012E 958
ADHG013I 958
ADHG014I 958
ADHG015W 958
ADHG017W 959
ADHG018I 959
ADHG019S 959
ADHG020I 959
ADHG021E 959

ADHG022I 959
ADHG026W 960
ADHG027I 960
ADHG030I 960
ADHG031I 960
ADHG097E 960
ADHG098I 960
ADHG099E 960
ADHG210I 961
ADHG501E 961
ADHG502E 961
ADHG503E 961
ADHG550E 961
ADHG510E 961
ADHG511E 962
ADHG512E 962
ADHG513E 962
ADHG514E 962
ADHG515E 962
ADHG516E 962
ADHG517E 963
ADHG520W 963
ADHG521W 963
ADHG522E 963
Error messages and codes: ADHIxxxx 963
ADHI026W 964
ADHI031I 964
ADHI530E 964
ADHI531W 964
ADHI612E 964
ADHI613E 964
ADHI697E 965
ADHI699E 965
Error messages and codes: ADHKxxxx 965
ADHK001I 965
ADHK002I 966
ADHK004I 966
ADHK005W 966
ADHK101I 966
ADHK102I 966
ADHK103I 966
ADHK104I 967
ADHK105I 967
ADHK106I 967
ADHK110I 967
ADHK111I 967
ADHK203I 967
ADHK204I 968
ADHK205I 968
Error messages and codes: ADHPxxxx 968
ADHP000I 970
ADHP001I 971
ADHP002I 971
ADHP003I 971
ADHP004W 971
ADHP005S 971
ADHP006E 971
ADHP007E 972
ADHP008S 972
ADHP009I 972
ADHP010I 972
ADHP012I 972
ADHP013I 972
ADHP015W 973
ADHP017W 973
ADHP018I 973
ADHP019S 973
ADHP020I 973
ADHP021E 973
ADHP022I 974
ADHP023I 974
ADHP026W 974

ADHP028E 974
ADHP030I 974
ADHP031I 974
ADHP093E 975
ADHP094E 975
ADHP095E 975
ADHP096E 975
ADHP097E 975
ADHP099E 975
ADHP101W 976
ADHP102E 976
ADHP110I 976
ADHP111I 976
ADHP120I 976
ADHP121I 976
ADHP122I 977
ADHP123I 977
ADHP124I 977
ADHP125I 977
ADHP126I 977
ADHP130I 977
ADHP131I 977
ADHP140I 978
ADHP141I 978
ADHP142I 978
ADHP143I 978
ADHP144I 978
ADHP145I 978
ADHP146I 979
ADHP150I 979
ADHP151I 979
ADHP160I 979
ADHP161I 979
ADHP162I 979
ADHP163I 979
ADHP164I 980
ADHP165I 980
ADHP166I 980
ADHP167I 980
ADHP168I 980
ADHP170I 980
ADHP179E 981
ADHP180I 981
ADHP183E 981
ADHP182I 981
ADHP183I 981
ADHP184I 981
ADHP185I 982
ADHP186I 982
ADHP188I 982
ADHP189W 982
ADHP190W 982
ADHP191W 982
ADHP192E 983
ADHP193I 983
ADHP200E 983
ADHP201E 983
ADHP203E 983
ADHP204E 983
ADHP205E 984
ADHP206E 984
ADHP207E 984
ADHP208E 984
ADHP209E 984
ADHP210I 984
ADHP211W 985
ADHP212W 985
ADHP213E 985
ADHP214E 985
ADHP215E 985
ADHP216W 985
ADHP217W 986

ADHP218W 986
ADHP220I 986
ADHP250E 986
ADHP550E 986
Error messages and codes: ADHQxxxx 986
ADHQ1000E 990
ADHQ1001I 991
ADHQ1002I 991
ADHQ1003E 991
ADHQ1004I 991
ADHQ1005I 991
ADHQ1006E 991
ADHQ1007E 992
ADHQ1010I 992
ADHQ1011I 992
ADHQ1016E 992
ADHQ1017E 992
ADHQ1019I 992
ADHQ1020E 993
ADHQ1024E 993
ADHQ1026E 993
ADHQ1027I 993
ADHQ1028E 993
ADHQ1031E 993
ADHQ1032I 994
ADHQ1033E 994
ADHQ1034I 994
ADHQ1035E 994
ADHQ1055E 994
ADHQ1060I 994
ADHQ1061E 995
ADHQ1062E 995
ADHQ1062I 995
ADHQ1065E 995
ADHQ1066E 995
ADHQ1070E 995
ADHQ1071E 996
ADHQ1080I 996
ADHQ1081I 996
POLICY PUSH DETECTED. 996
ADHQ1083I 996
ADHQ1084I 996
ADHQ1085I 997
ADHQ1086I 997
ADHQ1086E 997
ADHQ1153E 997
ADHQ1202I 997
ADHQ1203I 997
ADHQ1204I 998
ADHQ1205E 998
ADHQ1209I 998
ADHQ1210E 998
ADHQ1211I 998
ADHQ1212E 998
ADHQ1213W 999
ADHQ1214W 999
ADHQ1215W 999
ADHQ1216E 999
ADHQ1217W 1000
ADHQ1218W 1000
ADHQ1219W 1000
ADHQ1500E 1000
ADHQ2001E 1000
ADHQ2002E 1001
ADHQ2003I 1001
ADHQ2005I 1001
ADHQ2008E 1001
ADHQ2009E 1001
ADHQ2010I 1001
ADHQ2013I 1002
ADHQ2014I 1002
ADHQ2015I 1002

ADHQ2016I 1002
ADHQ2017I 1002
ADHQ2018I 1003
ADHQ2019I 1003
ADHQ2020I 1003
ADHQ2100E 1003
ADHQ2101E 1003
ADHQ2103E 1003
ADHQ2110E 1004
ADHQ2111E 1004
ADHQ2402I 1004
ADHQ2403I 1004
ADHQ2408E 1004
ADHQ2601E 1004
ADHQ2603E 1005
ADHQ3001I 1005
ADHQ3002I 1005
ADHQ3003I 1005
ADHQ3005I 1005
ADHQ3006I 1005
ADHQ3192E 1006
ADHQ3192I 1006
ADHQ3200I 1006
ADHQ3201I 1006
ADHQ3202I 1006
ADHQ3203I 1007
ADHQ3204I 1007
ADHQ3205I 1007
ADHQ3206I 1007
ADHQ3207I 1007
ADHQ3208I 1007
ADHQ3209I 1008
ADHQ3210I 1008
ADHQ3211I 1008
ADHQ3212I 1008
ADHQ3213I 1008
ADHQ3214I 1008
ADHQ3215I 1009
ADHQ3216I 1009
ADHQ3240I 1009
ADHQ3241I 1009
ADHQ3242I 1009
ADHQ3243I 1009
ADHQ3244I 1010
ADHQ3245I 1010
ADHQ3250I 1010
ADHQ3251I 1010
ADHQ3252I 1010
ADHQ3308E 1010
ADHQ3315E 1011
ADHQ3402I 1011
ADHQ3551E 1011
ADHQ3552E 1011
ADHQ3553E 1011
ADHQ4001E 1012
ADHQ4003E 1012
ADHQ5010I 1012
ADHQ5011I 1012
ADHQ5012I 1012
ADHQ5013I 1012
ADHQ6101E 1013
ADHQ6102E 1013
ADHQ7001E 1013
ADHQ7008E 1013
ADHQ7009E 1013
ADHQ7010E 1013
ADHQ7011E 1014
ADHQ7015E 1014
ADHQ7016E 1014
ADHQ8001E 1014
ADHQ8002E 1014
ADHQ8003E 1014

ADHQ8004E 1015
ADHQ8005E 1015
ADHQ8006E 1015
ADHQ8007E 1015
ADHQ8008E 1015
ADHQ8009E 1015
ADHQ8010E 1016
ADHQ8011E 1016
ADHQ8012E 1016
ADHQ8013E 1016
ADHQ8014E 1016
ADH8022I 1016
ADH9899I 1017
IBM Security Guardium S-TAP for IMS on z/OS 1017
IBM Security Guardium S-TAP for IMS on z/OS 1017
What does IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 do? 1017
What's new in IBM Security Guardium S-TAP for IMS on z/OS V10.1.3? 1018
IBM Guardium S-TAP for IMS components 1018
IBM Guardium system 1018
IBM Guardium S-TAP for IMS agent 1019
Installing IBM Security Guardium S-TAP for IMS on z/OS 1019
Hardware and software prerequisites 1019
User ID authorities that are required for installation 1019
IBM Security Guardium S-TAP for IMS on z/OS security 1019
APF authorization 1020
OMVS segment 1020
TCP/IP connections 1020
z/OS log streams 1020
IMS RESLIB data sets 1021
SMF and IMS archive log data sets 1021
DBRC RECON data sets 1021
Operator commands 1021
Quarantining Database DLI calls 1021
Configuration overview 1021
Upgrading from Guardium S-TAP for IMS V9.0 1022
Upgrading from Guardium S-TAP for IMS V9.1 or V10.0 1022
Planning your configuration and customizing your environment 1023
Customizing the ISPF edit macro 1023
Job cards for the sample JCL in the SAMPLIB 1024
Setting up z/OS log streams 1024
Log stream security 1024
XCF-based log streams 1024
DASD-based log streams 1026
Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent 1027
Customizing the agent configuration files 1027
Agent configuration 1035
Customizing the agent JCL 1035
Starting and stopping the agent 1035
Agent security considerations 1036
Modifying the frequency of AUIJ012I messages 1036
Setting up an IMS environment for auditing 1036
Security consideration for IMS processing 1036
Customizing IMS environments to capture DLI calls 1036
Customizing IMS cataloged procedures 1036
Coexisting with other DFSFLGX0 and DFSISVI0 Exit routines 1037
Defining LOGWRT exits 1037
Customizing IMS to use a System z Integrated Information Processor (ZzIIP) 1038
Copying common load modules from SAUILOAD to SAUIIMOD 1038
Configuring APP_EVENT support 1038
APP_EVENT examples 1038
Using agent configuration keywords 1039
Simulation mode 1041
Specifying multiple SMF data set masks 1041
Disabling SMF auditing at the agent level 1041
Controlling the frequency of SMF z/OS catalog queries 1042
Changing the retention period of incomplete SMF events 1042
Changing the name of the SMF address space JCL 1042
Auditing IMS data set access 1042
Changing the types of events that are audited using SMF records 1042
Using alternate RECON data sets for SMF and SLDS processing 1043
Overriding the range of ports used for communication between address space 1043
Overriding the TCP/IP DNS resolver table 1043

Specifying agent messages to issue to the operator console 1044
Creating a spill area for short-term outages 1044
Disabling IMS SLDS auditing at the agent level 1044
Controlling the frequency with which IMS System Log Data Sets are allocated and read 1045
Changing the name of the IMSL address space JCL 1045
Changing the types of events audited using IMS SLDS records 1045
Changing the name of the Common Memory Management address space JCL 1045
Excluding DLI calls on specific LPARS from being audited 1045
Running more than one agent in a SYSPLEX 1046
Restricting auditing to specific IMS systems when multiple IMS systems share RECON data sets 1046
Using the System z Integrated Information Processor (zIIP) 1046
Using multiple Guardium systems 1047
Providing Guardium system failover 1047
Streaming to multiple Guardium systems 1047
Keeping connections active when HOT_FAILOVER is enabled 1048
IBM Security Guardium S-TAP for IMS on z/OS agent reference information 1048
Sample library members 1048
Agent environment 1049
APF authorization 1049
Agent job output 1049
Stopping the agent 1049
Starting and stopping the secondary address spaces 1049
Data collection 1050
IMS database DLI calls 1050
SMF records 1050
Records from IMS system log data sets (SLDS) 1051
Filtering stages 1051
Stage 0 filtering 1052
Stage 1 filtering 1052
Stage 2 filtering 1052
Policy pushdown 1052
Creating and modifying IMS definitions 1053
Navigating to the IMS Definitions panel 1053
IMS Definition fields 1053
IMSPLEX data sharing and XRF considerations 1054
Adding an IMS definition 1054
Modifying an IMS definition 1054
Deleting an IMS definition 1054
Reference information 1055
Data collection monitors 1055
IMS Logtypes and SMF record types that are collected by InfoSphere Guardium S-TAP for IMS 1056
Fields that are used for IMS policy pushdown 1057
Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS 1058
Calculating the Optimal Log Stream Size 1058
Considerations 1058
Using IBM Documentation 1059
Pertinent Report Fields 1059
Additional Resources 1059
XML statement definitions 1059
Sample XML file 1062
AUIA060W 1063
Troubleshooting 1063
Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS 1063
Error messages and codes: AUIAxxxx 1064
AUIA003E 1065
AUIA004E 1065
AUIA005I 1065
AUIA006I 1065
AUIA007I 1065
AUIA008I 1066
AUIA009E 1066
AUIA010E 1066
AUIA021I 1066
AUIA022I 1066
AUIA023I 1066
AUIA024I 1067
AUIA027E 1067
AUIA028S 1067
AUIA029I 1067
AUIA030I 1067
AUIA031I 1068
AUIA033I 1068

AUIA034S 1068
AUIA035W 1068
AUIA036I 1068
AUIA037I 1068
AUIA038S 1068
AUIA041I 1069
AUIA042W 1069
AUIA043I 1069
AUIA044I 1069
AUIA045I 1069
AUIA048I 1069
AUIA049W 1070
AUIA050W 1070
AUIA051I 1070
AUIA052I 1070
AUIA053I 1071
AUIA054I 1071
AUIA055I 1071
AUIA056I 1071
AUIA057I 1071
AUIA058I 1071
AUIA059I 1072
AUIA060W 1072
AUIA061I 1072
Error messages and codes: AUIBxxxx 1072
AUIB300I 1073
AUIB302I 1073
AUIB305I 1073
AUIB306E 1073
AUIB700I 1074
Error messages and codes: AUIFxxxx 1074
AUIF002I 1074
AUIF003E 1074
AUIF501I 1075
AUIF502I 1075
AUIF503I 1075
AUIF505I 1075
AUIF506I 1075
AUIF507E 1076
AUIF508I 1076
AUIF702I 1076
Error messages and codes: AUIGxxxx 1076
AUIG001S 1077
AUIG002S 1077
AUIG003S 1077
AUIG004S 1077
AUIG005S 1078
AUIG006S 1078
AUIG014E 1078
AUIG015W 1078
AUIG016S 1078
AUIG017S 1079
AUIG018S 1079
AUIG045E 1079
AUIG046E 1079
AUIG047E 1079
AUIG048E 1079
AUIG049E 1080
AUIG050E 1080
AUIG051I 1080
AUIG052I 1080
AUIG053I 1080
AUIGF120I 1081
AUIGF201I 1081
AUIGF202I 1081
Error messages and codes: AUIIxxxx 1081
AUII017I 1082
AUII018E 1083
AUII019E 1083
AUII020E 1083
AUII021E 1083
AUII022E 1083

AUII023E 1084
AUII024E 1084
AUII025E 1084
AUII026E 1084
AUII027E 1084
AUII028E 1085
AUII029E 1085
AUII031E 1085
AUII038E 1085
AUII040E 1086
AUII041E 1086
AUII042W 1086
AUII043W 1086
AUII044E 1086
AUII046E 1087
AUII049E 1087
AUII050I 1087
AUII052I 1088
AUII055I 1088
AUII056I 1088
AUII057I 1088
AUII058A 1088
AUII060W 1089
AUII061I 1089
AUII120I 1089
AUII172I 1089
AUII173E 1090
AUII174E 1090
AUII175I 1090
AUII176E 1090
AUII177E 1090
AUII178E 1091
Error messages and codes: AUIJxxxx 1091
AUIJ005W 1093
AUIJ006E 1093
AUIJ007E 1093
AUIJ008I 1093
AUIJ009E 1093
AUIJ010I 1094
AUIJ011I 1094
AUIJ012I 1094
AUIJ013E 1095
AUIJ014E 1095
AUIJ015E 1095
AUIJ016E 1095
AUIJ017I 1095
AUIJ018W 1096
AUIJ019E 1096
AUIJ020I 1096
AUIJ021W 1096
AUIJ022W 1096
AUIJ023E 1097
AUIJ024W 1097
AUIJ042W 1097
AUIJ044W 1097
AUIJ055I 1098
AUIJ056I 1098
AUIJ057W 1098
AUIJ058W 1098
AUIJ201E 1098
AUIJ202E 1099
AUIJ203E 1099
AUIJ250I 1100
AUIJ251E 1100
AUIJ252W 1100
AUIJ255I 1100
AUIJ256I 1101
AUIJ257I 1101
AUIJ258I 1101
AUIJ259I 1101
AUIJ303W 1101
AUIJ304A 1102

AUIJ304E 1102
AUIJ307A 1102
AUIJ307E 1102
AUIJ330E 1103
AUIJ331E 1103
AUIJ332E 1103
AUIJ333E 1103
AUIJ335W 1104
AUIJ400E 1104
AUIJ401E 1104
AUIJ402E 1104
AUIJ403E 1104
AUIJ404E 1105
AUIJ406W 1105
AUIJ407I 1105
AUIJ408E 1105
AUIJ500I 1106
AUIJ501I 1106
AUIJ504I 1106
AUIJ521W 1106
AUIJ510I 1107
AUIJ511E 1107
AUIJ512E 1107
AUIJ513E 1107
AUIJ522E 1107
AUIJ609I 1108
AUIJ800E 1108
AUIJ860E 1108
AUIJ999E 1108
Error messages and codes: AUILxxxx 1109
AUIL002I 1109
AUIL003E 1109
AUIL600I 1109
AUIL601I 1109
AUIL602I 1110
AUIL603I 1110
AUIL605I 1110
AUIL606W 1110
AUIL607W 1111
AUIL701I 1111
Error messages and codes: AUIPxxxx 1111
AUIP001E 1112
AUIP002E 1112
AUIP003E 1112
AUIP004E 1112
AUIP005E 1112
AUIP006S 1112
AUIP007E 1113
AUIP008E 1113
AUIP009E 1113
AUIP010E 1113
AUIP011E 1113
AUIP012E 1114
AUIP013E 1114
AUIP014E 1114
AUIP015E 1114
AUIP016E 1114
Error messages and codes: AUIRxxxx 1114
AUIR002E 1115
AUIR004E 1115
AUIR006E 1115
AUIR007W 1115
AUIR008W 1115
Error messages and codes: AUITxxxx 1115
AUIT001E 1116
AUIT006S 1116
AUIT008E 1116
AUIT010E 1117
AUIT012I 1117
AUIT013I 1117
AUIT014I 1117
AUIT015I 1117

AUIT017I 1117
AUIT019I 1118
AUIT020I 1118
AUIT023I 1118
AUIT025I 1118
AUIT028E 1118
AUIT031I 1118
AUIT032I 1119
AUIT033I 1119
AUIT034S 1119
AUIT044E 1119
AUIT047E 1119
AUIT048I 1119
AUIT049I 1120
Error messages and codes: AUIUxxxx 1120
AUIUR002I 1120
AUIUR003I 1120
Error messages and codes: AUIXxxxx 1120
AUIX013E 1123
AUIX014E 1123
AUIX015E 1123
AUIX016E 1123
AUIX017E 1123
AUIX018E 1124
AUIX019E 1124
AUIX020E 1124
AUIX021E 1124
AUIX022E 1124
AUIX023E 1124
AUIX024E 1125
AUIX025E 1125
AUIX026E 1125
AUIX027S 1125
AUIX028E 1125
AUIX034S 1125
AUIX035E 1126
AUIX036E 1126
AUIX037E 1126
AUIX038E 1126
AUIX039E 1126
AUIX040E 1126
AUIX041E 1127
AUIX042E 1127
AUIX043E 1127
AUIX044E 1127
AUIX045E 1127
AUIX046E 1127
AUIX047E 1128
AUIX048E 1128
AUIX049E 1128
AUIX050E 1128
AUIX051E 1128
AUIX052E 1128
AUIX053E 1129
AUIX054E 1129
AUIX055E 1129
AUIX056E 1129
AUIX057E 1129
AUIX058E 1129
AUIX059E 1130
AUIX060E 1130
AUIX061S 1130
AUIX062E 1130
AUIX063E 1130
AUIX064E 1131
AUIX066E 1131
AUIX067E 1131
AUIX068E 1131
AUIX074E 1131
AUIX076E 1131
AUIX085E 1132
AUIX086E 1132

AUIX087E 1132
AUIX088E 1132
AUIX093S 1132
AUIX094S 1132
AUIX095S 1133
AUIX096S 1133
AUIX097S 1133
AUIX098E 1133
AUIX101E 1133
AUIX104E 1133
AUIX109E 1134
AUIX110I 1134
AUIX114E 1134
AUIX115E 1134
AUIX116I 1134
AUIX122I 1135
AUIX123W 1135
AUIX124S 1135
AUIX126E 1135
AUIX127S 1135
AUIX142E 1135
AUIX143E 1136
AUIX149E 1136
AUIX150E 1136
AUIX151E 1136
AUIX152E 1136
AUIX153E 1136
AUIX154E 1137
AUIX155E 1137
AUIX156E 1137
AUIX160E 1137
AUIX183E 1137
Error messages and codes: AUIYxxxx 1137
AUIY001E 1138
AUIY002E 1138
AUIY003E 1138
AUIY004E 1138
AUIY005E 1138
AUIY006E 1139
AUIY007I 1139
AUIY008I 1139
AUIY009E 1139
Error messages and codes: AUIZxxxx 1139
AUIZ002E 1141
AUIZ003W 1141
AUIZ004S 1141
AUIZ005S 1141
AUIZ007S 1142
AUIZ008W 1142
AUIZ009S 1142
AUIZ010W 1142
AUIZ011W 1142
AUIZ012I 1142
AUIZ013E 1143
AUIZ014W 1143
AUIZ020W 1143
AUIZ021E 1143
AUIZ022E 1143
AUIZ023E 1144
AUIZ024E 1144
AUIZ025E 1144
AUIZ026E 1144
AUIZ027W 1144
AUIZ028E 1144
AUIZ029E 1145
AUIZ030E 1145
AUIZ031E 1145
AUIZ032E 1145
AUIZ033E 1145
AUIZ034E 1145
AUIZ035E 1146
AUIZ036E 1146

AUIZ037I 1146
AUIZ038I 1146
AUIZ039I 1146
AUIZ040I 1146
AUIZ041E 1147
AUIZ041W 1147
AUIZ042W 1147
AUIZ043E 1147
AUIZ044S 1147
AUIZ045E 1148
AUIZ046E 1148
AUIZ047E 1148
AUIZ048E 1148
AUIZ049E 1148
AUIZ050E 1148
AUIZ051E 1149
AUIZ052E 1149
AUIZ053E 1149
AUIZ054E 1149
AUIZ055E 1149
AUIZ056E 1150
AUIZ057E 1150
AUIZ058I 1150
AUIZ059E 1150
AUIZ060E 1150
AUIZ061I 1151
AUIZ062I 1151
AUIZ063E 1151
AUIZ064E 1151
AUIZ065W 1152
AUIZ066E 1152
AUIZ067W 1152
IBM Security Guardium S-TAP for Data Sets on z/OS 1152
IBM Security Guardium S-TAP for Data Sets on z/OS overview 1153
What's new in IBM Guardium S-TAP for Data Sets V10.1.3? 1153
IBM Guardium S-TAP for Data Sets components 1153
Installation requirements for IBM Guardium S-TAP for Data Sets V10.1.3 1154
Software prerequisites 1154
User ID authority requirements 1154
Configuring the IBM Guardium S-TAP for Data Sets agent 1154
Security 1155
APF authorizing the load library 1155
Authorizing the z/OS agent started task for the control data set 1155
Defining an OMVS segment 1156
Planning your configuration 1156
Job cards for the sample JCL in the sample library 1156
Allocating auxiliary storage 1156
Configuring the SMFPRMxx PARMLIB member 1156
IAM and ACF2 collection considerations 1157
Enabling Innovations Data Processing IAM reporting 1157
Enabling Computer Associates International ACF2 reporting 1157
Creating the control data set 1157
Specifying subsystem options 1158
Configuring the started task JCL 1161
CICS Transaction Server support 1161
Configuring CICS Transaction Server support 1161
Using CICS system initialization parameters 1163
Configuring CICS signon reporting 1163
Starting the product 1164
Starting and stopping the agent started task 1164
Sample library members 1164
Verifying the installation 1164
IBM Guardium S-TAP for Data Sets administration 1165
Communicating with the Guardium system 1166
Streaming audit data to multiple systems 1166
Keeping connections active when HOT_FAILOVER is enabled 1166
Communicating with the IBM Guardium S-TAP for Data Sets started task 1166
IBM Guardium S-TAP for Data Sets started task commands 1166
Data collection 1167
Record level and SMF data set monitoring options 1169
Policy pushdown 1171
Data set collection filtering parameters 1171

CICS collection filtering parameters 1176
Reference information 1177
Simulation mode 1177
VSAM and non-VSAM data set types and events 1178
SMF record types 1179
Time-to-reporting considerations 1180
Troubleshooting 1180
Messages and codes 1180
Error message code descriptions 1181
AUV1001I 1186
AUV1002E 1186
AUV1003E 1186
AUV1004E 1186
AUV1005E 1186
AUV1006E 1187
AUV1007E 1187
AUV1008I 1187
AUV1009E 1187
AUV1012E 1187
AUV1013I 1187
AUV1014E 1188
AUV1015E 1188
AUV1016E 1188
AUV1017I 1188
AUV1018E 1188
AUV1019I 1188
AUV1020E 1189
AUV1021E 1189
AUV1022E 1189
AUV1023E 1189
AUV1024I 1189
AUV1025E 1189
AUV1026I 1190
AUV1027E 1190
AUV1028I 1190
AUV1029E 1190
AUV1030I 1190
AUV1031E 1190
AUV1032I 1191
AUV1033E 1191
AUV1034E 1191
AUV1035E 1191
AUV1036E 1191
AUV1038E 1191
AUV1040E 1191
AUV1041I 1192
AUV1042E 1192
AUV1043E 1192
AUV1044E 1192
AUV1046E 1192
AUV1047E 1192
AUV1048I 1193
AUV1049E 1193
AUV1050E 1193
AUV1052E 1193
AUV1054E 1193
AUV1055E 1194
AUV1056I 1194
AUV1058E 1194
AUV1058I 1194
AUV1059E 1194
AUV1060I 1194
AUV1061E 1195
AUV1062I 1195
AUV1063E 1195
AUV1064W 1195
AUV1065E 1195
AUV1066E 1195
AUV1067E 1196
AUV1068E 1196
AUV1069E 1196
AUV1070I 1196

AUV1073W 1196
AUV1074E 1196
AUV1077I 1197
AUV1080E 1197
AUV1081E 1197
AUV1082W 1197
AUV1100E 1197
AUV1101E 1198
AUV1102E 1198
AUV1103E 1198
AUV1105E 1198
AUV1105I 1198
AUV1106I 1198
AUV1107I 1199
AUV1111E 1199
AUV1112E 1199
AUV1113E 1199
AUV1115E 1199
AUV1116E 1200
AUV1117E 1200
AUV1122E 1200
AUV1123E 1200
AUV1123W 1200
AUV1124E 1200
AUV1125E 1200
AUV1126E 1201
AUV1127I 1201
AUV1128E 1201
AUV1129I 1201
AUV1130I 1201
AUV1131I 1201
AUV1132I 1202
AUV1136I 1202
AUV1137I 1202
AUV1138E 1202
AUV1140I 1202
AUV1141I 1202
AUV1142I 1203
AUV1143I 1203
AUV1144I 1203
AUV1145I 1203
AUV1146E 1203
AUV1147I 1203
AUV1149I 1204
AUV1150I 1204
AUV1151E 1204
AUV1152I 1204
AUV1153I 1204
AUV1154E 1204
AUV1155E 1205
AUV1156E 1205
AUV1157E 1205
AUV1158E 1205
AUV1175I 1205
AUV1176E 1205
AUV1176I 1206
AUV1177I 1206
AUV1179E 1206
AUV1184E 1206
AUV1185E 1206
AUV1191E 1206
AUV1192I 1207
AUV1193I 1207
AUV1195E 1207
AUV1196E 1207
AUV1200E 1207
AUV1202E 1208
AUV1203E 1208
AUV1204E 1208
AUV1213E 1208
AUV1214E 1208
AUV1215E 1208

AUV1400I 1208
AUV1401I 1209
AUV1402I 1209
AUV1405I 1209
AUV1406W 1209
AUV1408W 1209
AUV1410I 1210
AUV1411E 1210
AUV1412I 1210
AUV1413E 1210
AUV1414I 1210
AUV1415E 1210
AUV1416I 1211
AUV1417E 1211
AUV1418I 1211
AUV1419E 1211
AUV1420I 1211
AUV1421E 1211
AUV1422I 1212
AUV1423E 1212
AUV1424I 1212
AUV1425E 1212
AUV1438I 1212
AUV1439I 1213
AUV1450W 1213
AUV1747E 1213
AUV1748W 1213
AUV2000E 1213
AUV2030E 1214
AUV2040E 1214
AUV2041E 1214
AUV2042E 1214
AUV2097I 1214
AUV2098I 1214
AUV2104E 1215
AUV2170I 1215
AUV2171I 1215
AUV2172E 1215
AUV2173E 1215
AUV2174E 1216
AUV2175E 1216
AUV2176E 1216
AUV2177E 1216
AUV2178I 1216
AUV2179E 1217
AUV2180W 1217
AUV2181I 1217
AUV2182I 1217
AUV2183W 1217
AUV2184W 1217
AUV2185I 1218
AUV2186E 1218
AUV2900E 1218
AUV2901E 1218
AUV2902E 1218
AUV2903E 1218
AUV3000E 1219
AUV3001E 1219
AUV3003E 1219
AUV3004I 1219
AUV3005E 1219
AUV3006E 1219
AUV3008E 1220
AUV3009I 1220
AUV3010W 1220

IBM Security Guardium V10.1

Bienvenido a la documentación de IBM Security Guardium, donde encontrará información acerca de cómo instalar, mantener y utilizar IBM Guardium.

Guía de inicio

Visión general del producto
Avisos legales del producto
Novedades
Notas del release
Instalación
Actualización

Tareas comunes

Descubrimiento de datos confidenciales
Supervisión del estado de despliegue
Supervisión del estado de S-TAP
Distribución de los perfiles de configuración
Gestión de roles y permisos

Resolución de problemas y soporte

Inicio de soporte de Guardium
Recursos de soporte de Guardium
Vídeos de soporte de Guardium
Respuesta de IBM developerWorks para Guardium

Más información

IBM Security Learning Academy
Seguridad de datos y protección de IBM
Comunidad de Guardium de IBM developerWorks
Vídeos de Guardium

© Copyright IBM Corp. 2002, 2017

Visión general del producto

Información del producto y release de Guardium Solutions.

- IBM Guardium
  IBM Guardium protege antes fugas en bases de datos, almacenes de datos y entornos de Big Data como, por ejemplo, Hadoop, garantiza la integridad de la información y automatiza el cumplimento de controles a través de entornos heterogéneos.
- Novedades de este release
  Nuevas características, funciones y mejoras.
- Notas del release
  Conozca las últimas características y mejoras, los requisitos del sistema y la información de actualización, instalación y soporte.

IBM Guardium

IBM Guardium protege antes fugas en bases de datos, almacenes de datos y entornos de Big Data como, por ejemplo, Hadoop, garantiza la integridad de la información y automatiza el cumplimento de controles a través de entornos heterogéneos.

Protege datos estructurados y no estructurados en bases de datos, entornos de Big Data y sistemas de archivos frente a las amenazas y garantiza el cumplimiento normativo.

Proporciona una plataforma escalable que permite la supervisión continua del tráfico de datos estructurados y no estructurados, así como el cumplimiento de políticas para el acceso a datos confidenciales en toda la empresa.

Un repositorio de auditoría seguro y centralizado combinado con una plataforma de automatización de flujo de trabajo integrada agiliza las actividades de validación en una amplia variedad de mandatos.

Aprovecha la integración con la gestión de la TI y de otras soluciones de gestión de la seguridad para proporcionar una protección integral de los datos en toda la empresa.

La solución está diseñada para permitir la supervisión continua de infraestructuras de compartición de documentos y bases de datos heterogéneas, así como el cumplimiento de las políticas para el acceso a datos confidenciales en toda la empresa, utilizando una plataforma escalable. El repositorio de auditoría centralizado está diseñado para maximizar la seguridad, combinado con una aplicación de automatización de flujo de trabajo de cumplimiento integrado que facilita a los productos realizar las actividades de validación de conformidad en una amplia variedad de mandatos.

IBM Security Guardium está diseñado para proteger datos críticos. Guardium es una plataforma completa de protección de datos que permite a los equipos de seguridad analizar automáticamente lo que sucede en entornos de datos confidenciales (bases de datos, almacenes de datos, plataformas de Big Data, entornos en la nube, sistemas de archivos, etc.) para ayudar a minimizar el riesgo, proteger los datos confidenciales de amenazas internas y externas, y adaptarse perfectamente a los cambios de TI que puedan afectar a la seguridad de los datos. Guardium ayuda a garantizar la integridad de la información en los centros de datos y a automatizar los controles de cumplimiento.

La solución de IBM Security Guardium se ofrece en dos versiones:

- IBM Security Guardium Database Activity Monitoring (DAM)
- IBM Security Guardium File Activity Monitoring (FAM) - Utilice la supervisión de actividad de archivos de Guardium para ampliar las funcionalidades de supervisión a los servidores de archivos.

Los productos de IBM Guardium proporcionan una solución simple y robusta para evitar fugas de datos de bases de datos y archivos, lo que ayuda a garantizar la integridad de la información en el centro de datos y a automatizar los controles de cumplimiento.

Los productos de Guardium pueden ayudarle a:

- Encontrar de forma automática bases de datos y descubrir y clasificar información confidencial dentro de las mismas.
- Asesorar de forma automática con relación a debilidades de configuración y vulnerabilidades de la base de datos.
- Asegurarse de que las configuraciones quedan protegidas después de que se implementen los cambios recomendados.
- Habilitar una alta visibilidad a un nivel granular en las transacciones de base de datos que implican datos confidenciales.
- Realizar un seguimiento de las actividades de los usuarios finales que acceden a datos indirectamente a través de aplicaciones empresariales.
- Supervisar y aplicar una amplia gama de políticas, incluidas algunas relacionadas con el acceso a datos confidenciales, control de cambios de base de datos y acciones de usuarios privilegiados.
- Crear un único repositorio de auditoría centralizado seguro para un gran número de bases de datos y sistemas.
- Automatizar todo el proceso de auditoría de cumplimiento, incluida la creación y distribución de informes así como la captura de comentarios y firmas.

La solución Guardium se ha diseñado para facilitar se uso y proporcionar escalabilidad. Se puede configurar tanto para una base de datos individual como para miles de bases de datos heterogéneas ubicadas por toda la empresa.

La solución está disponible en forma de dispositivos preconfigurados que IBM® entrega o en forma de dispositivos de software instalados en su plataforma. Existen características opcionales que se pueden añadir fácilmente al sistema después de la instalación.

Estas son las áreas funcionales más importantes de la solución de seguridad de bases de datos de Guardium:

- Asesoramiento de vulnerabilidades. Incluye no solo el descubrimiento de vulnerabilidades conocidas en productos de base de datos, sino que también proporciona una visibilidad completa de infraestructuras de bases de datos complejas, detecta errores de configuración y asesora y mitiga con relación a estos riesgos.
- Clasificación y descubrimiento de datos. Aunque la clasificación por sí sola no proporciona ninguna protección, sirve como un primer paso crucial para definir políticas de seguridad adecuadas para distintos datos en función de su importancia y de los requisitos de cumplimiento.
- Protección de datos. Guardium se encarga del cifrado de los datos tanto de forma estática como en su tránsito, proporciona enmascaramiento de datos de forma dinámica y estática. También utiliza otras tecnologías para proteger la integridad y confidencialidad de los datos.
- Supervisión y analíticas. Incluye la supervisión de las características de rendimiento de la base de datos y la visibilidad completa de todas las acciones de administración y de acceso para cada instancia. Por encima de este nivel, puede proporcionar analíticas avanzadas en tiempo real, información de seguridad y de detección de anomalías y gestión de sucesos (SIEM).
- Prevención de amenazas. Hace referencia a los métodos de protección frente a ataques cibernéticos como, por ejemplo, los de denegación de servicio distribuido (DDoS) o inyección SQL, mitigación de vulnerabilidades no corregidas y otras medidas de seguridad específicas de cada base de datos.
- Gestión de accesos. Va más allá de los controles de acceso básicos a las instancias de base de datos. El proceso de valoración se centra en una gestión de acceso dinámico más sofisticado basado en políticas que es capaz de identificar y eliminar privilegios de usuario excesivos, gestionar cuentas de servicio y compartidas y de detectar y bloquear actividades sospechosas de los usuarios.
- Auditoría y cumplimiento. Incluye mecanismos avanzados de auditoría más allá de las funcionalidades nativas, auditoría centralizada e informes en varios entornos de base de datos, imposición de la separación de tareas y herramientas que dan soporte a los análisis forenses y las auditorías de cumplimiento.
- Rendimiento y escalabilidad. Aunque no es una característica de seguridad por se, es un requisito crucial de todas las soluciones de seguridad de bases de datos el que puedan resistir altas cargas, minimizando la sobrecarga en el rendimiento y dando soporte a los despliegues en configuraciones de alta disponibilidad.

Para obtener más información sobre la familia de productos de Guardium, visite http://www.ibm.com/software/data/guardium/.

Tema principal: Visión general del producto

Novedades de este release

Nuevas características, funciones y mejoras.

IBM Security Guardium V10.1.4

Supervisión de Amazon Oracle v11 RDS DBaaS utilizando la integración de auditoría nativa

Inhabilitación de TLS1.0/1.1, habilitación de TLS1.2

Soporte VA Oracle 12.2

Interfaz gráfica de usuario de VA para mostrar descripciones breves

Actualización de OpenSSL para S-TAP de Windows/UNIX

Soporte para EMC ATMOS

Acelerador de GDPR para z/OS

Mejoras en el clasificador

Despliegue simplificado de S-TAP a través de GIM

Nueva versión de interfaz gráfica de usuario del Creador de grupos

Mejoras en el equilibrador de carga empresarial para verificar que el sniffer está activo antes de asignar unidades gestionadas

Permitir múltiples almacenamientos intermedios KTAP con más de cinco recopiladores

Priorización de paquetes de conexión respecto a los paquetes normales

IBM Security Guardium V10.1.3

Inicio rápido para la supervisión del cumplimiento

- Despliegue de agentes de supervisión: Permite prepararse rápidamente para la supervisión de bases de datos descubriendo y activando clientes de GIM, instalando S-TAP, creando motores de inspección y correlacionando los S-TAP con los recopiladores.
- Configuración de la supervisión de cumplimiento: Ayuda a cumplir los estándares de cumplimiento mediante la instalación rápida de políticas, la creación de grupos y la ejecución de informes para supervisar la actividad de la base de datos.

Cloudera Hadoop: El sistema Guardium fue el primero en proporcionar asesoramiento de vulnerabilidades (VA) en el espacio No SQL con su soporte a MongoDB. Ahora Guardium se amplía hasta el espacio Hadoop/Big Data con soporte para la plataforma Cloudera. Guardium Vulnerability Assessment permite a las organizaciones sentirse más confiadas en el uso de Cloudera ofreciendo asesoramiento y un correcto funcionamiento del sistema para alinearlo con los procedimientos de seguridad recomendados. Combinado con Guardium Activity Monitor para auditorías en tiempo real, ejecución de cumplimientos y analíticas de seguridad, Guardium puede proporcionar una solución de seguridad global para Cloudera y para la mayoría de bases de datos y almacenes de datos en entornos empresariales típicos.

Guardium S-TAP for z/OS: IBM Security Guardium, amplía la seguridad de los datos en sistemas principales con una mejor:

- Protección de datos para bloquear actividades de usuario no autorizadas en DB2 for z/OS
- Rendimiento y optimización para reducir sobrecargas
- Funciones de auditoría y filtrado para ampliar más la protección de datos y las analíticas en tiempo real
- Usabilidad y soportabilidad para acelerar el despliegue y los diagnósticos

IBM Security Guardium V10.1.2

1. Mejoras en la detección de valores atípicos

   Un valor atípico lo define un comportamiento de un origen determinado (una base de datos, un usuario determinado en una base de datos, un servidor o un usuario de SO) en un periodo de tiempo determinado que está fuera del marco temporal "normal" o del ámbito de la actividad de dicho origen. La detección de valores atípicos amplía la supervisión tradicional de bases de datos con una mayor inteligencia y que proporciona una detección temprana de posibles ataques durante el análisis de los cambios en el comportamiento de los orígenes. Este release introduce:

   - Soporte FAM
   - Ejecución en un agregador de datos desde varios recopiladores
   - Página de estado de minería de valores atípicos, que proporciona el estado actual del proceso de minería de valores atípicos en todas las unidades gestionadas y permite profundizar en el proceso de valores atípicos que no se han completado de forma satisfactoria.
   - Dos separadores en la Tabla de resultados del Panel de control de investigación: Un separador de Resumen con una fila por origen por hora en el que se encontró una anomalía, con una puntuación de anomalía y las razones de la misma; un separador de Detalles tiene una fila por valor atípico con la puntuación de anomalía y las razones y detalles (programa de origen, objeto, verbo, etc.).

2. Mejoras en la supervisión de la actividad de Hadoop con integración de Cloudera 5.7+ / Ranger

   Este release amplía el soporte de Guardium para supervisar Hadoop con integración Cloudera mediante la integración de Cloudera Navigator y Hortonworks utilizando Apache Ranger. Estas integraciones permiten el cifrado SSL para clientes que necesitan acceder a datos de Hadoop mediante la nueva interfaz de usuario de supervisión de Hadoop.

3. Mejoras en el clasificador y opción de archivado/copia de seguridad de Cleversafe

   Guardium ahora da soporte a la ejecución simultánea de varios procesos de clasificador. La posibilidad de ejecutar más de un proceso de clasificador a la vez permite un uso más eficaz de los recursos de CPU del sistema.

   De forma predeterminada, los procesos de clasificador de Guardium ahora excluyen varias bases de datos y esquemas utilizados por los proveedores de software. Al excluir estas bases de datos y tablas, los procesos de clasificación se ejecutan de forma más eficaz y devuelven menos errores.

   El archivado/copia de seguridad de Cleversafe da soporte a la interfaz Amazon S3 mediante el mismo SDK. La interfaz de Guardium para Cleversafe es análoga a la de Amazon S3 (a la que Guardium también da soporte). El soporte de Guardium incluye ahora Cleversafe, SoftLayer y Amazon S3.

4. Vistas de salud empresarial

   El nuevo panel de control de Salud del despliegue amplía las vistas de salud de despliegue existentes proporcionando un resumen global de los problemas de salud en todo el despliegue de Guardium. El panel de control es especialmente útil para identificar patrones y tendencias en los datos de salud antes de investigar sistemas individuales en los que se identifican problemas.

5. Mejoras de FAM: encadenamiento de UID, reglas de múltiples y valores atípicos

   Cadena de UID de Windows FAM: Actualmente, el agente Windows FAM devuelve el nombre de usuario del proceso asignado a un suceso de archivo. Ahora, el agente Windows FAM cambiará ese nombre de usuario individual por una cadena de nombres de usuario que pertenezcan al historial del proceso (cadena de UID). Por ejemplo, un Proceso 1 (usuario janedoe) crea un Proceso 2 (user johndoe), entonces, para los sucesos de archivo relacionados con el proceso 2, FAM informará que la cadena de UID está formada por {janedoe, johndoe}.

   Regla de múltiples acciones para FAM: Las reglas de múltiples acciones comprenden varias acciones, cada una para una categoría de mandato especifica o un grupo específico. Los mandatos en un contexto de FAM son: Leer, Escribir, Suprimir, Ejecutar y Operación de archivo.

6. Optimización de titularidades

   La optimización de titularidades media entre el rol del DBA proporcionando a los usuarios las titularidades necesarias para realizar sus trabajos de forma eficiente, y el rol de Seguridad para mantener las titularidades adecuadas y lo más restringidas posible para evitar vulnerabilidades en el sistema. Navegue hasta la optimización de titularidades con Descubrir > Titularidades de base de datos > Optimización de titularidades

7. Soporte de HP Vertica

   HP Vertica es un sistema de Big Data que compite con Hadoop. HP-Vertica proporciona una interfaz SQL Postgres estándar con sus extensiones propietarias.

   HP Vertica se utiliza en almacenes de datos con el fin de proporcionar un rendimiento de consultas muy rápido. HP Vertica se utiliza para el análisis de interacción de usuarios, el seguimiento de anuncios, las aplicaciones de corrientes de pulsaciones de usuario, el asesoramiento de amenazas y las predicciones financieras.

8. Cambios en los RPM de UNIX S-TAP

   - Instalación en /opt/guardium (la ubicación no se puede cambiar).
   - Configuración predeterminada de RPM

   ktap_installed=1

   La carga flexible se puede utilizar exportando NI_ALLOW_MODULE_COMBOS="Y" antes de la instalación de RPM

   sqlguard_ip establecido en 127.0.0.1

   tap_ip establecido en hostname

   Los registros de RPM guardados en /opt/guardium/rpm_logs

   - La actualización dinámica está soportada.

   Se da soporte a actualizaciones de solicitudes KTAP a través de procesos existentes (incrementa la versión de paquete).

   - Los instaladores de shell y GIM se rehusarán ser instalados si se detecta la instalación de RPM.
   - STAP se ejecutará después de la instalación, pero será necesario realizar la configuración.
   - Se proporciona un nuevo script, guard-config-update, para facilitar la configuración posterior a la instalación.

9. Acelerador de GDPR

   La seguridad y la privacidad de los datos son dos de las preocupaciones más importantes a las que debe enfrentarse cualquier organización. Previamente dentro de la Unión Europea cada país imponía diferentes niveles de cumplimiento, ahora el nuevo Reglamento General de Protección de Datos (GPDR - General Data Protection Regulation) amplia y establece estándares para las reglas de protección de datos a través de toda la Unión Europea.

   El acelerador Guardium GDPR proporciona informes predefinidos basados en políticas y grupos de GDPR. Para empezar a trabajar con el acelerador de GDPR, asigne el rol GDPR a un usuario de Guardium y, a continuación, vaya a Aceleradores > GDPR con dicha cuenta de usuario.

10. Visión de datos

    La visión de datos presenta un paradigma revolucionario que utiliza funcionalidades visuales humanas para obtener una visión global del flujo de datos para identificar comportamientos inesperados. Guardium ya proporciona sólidas características de análisis de datos y aprendizaje máquina para ayudar en auditorías y para detectar ataques en función de la experiencia y el conocimiento acumulados. La visión de datos añade la flexibilidad de la percepción visual humana para detectar asociaciones y traspasos en los datos, independientemente del tipo de ataque, que de lo contrario no serían advertidos.

    Por ejemplo, un proyecto de reconocimiento de objetos para identificar los baches en las calles de la ciudad podrían no identificar un objeto de gran tamaño en las vecindades. El ojo humano, sin embargo, lo detectaría de forma inmediata. De forma similar, al revisar datos auditados en diagramas de barras, los usuarios buscan tipos de problemas conocidos, pero pueden pasar por alto fácilmente aberraciones nuevas (desconocidas).

    La visión de datos convierte datos auditados en una visualización cronológica en 3-D de los orígenes y destinos de datos, mostrando como se van realizando las transacciones exactamente tal como se producen.

    El espacio de visualización contiene dos planos, cada uno de ellos representa entidades del dominio de auditoría de un tipo determinado. Cada entrada de los datos de auditoría se representa como una 'línea parpadeante' desde un objeto del plano superior (dirección IP de cliente, usuario de SO, usuario de base de datos, programa fuente) a un objeto en el plano inferior (base de datos, objeto, servidor). La línea parpadeante entre el origen y el destino deja un camino (una línea punteada) que indica la presencia de la interacción entre el origen y el destino específicos, que gradualmente se desvanece en el fondo. Los caminos proporcionan una visión general de la interacción entre los orígenes y los destinos en el periodo de tiempo seleccionado. Los orígenes están ubicados cerca de sus destinos y cerca de otros orígenes similares. El tamaño de la entidad de destino es proporcional al volumen de transacciones en relación con las otras entidades de destino. Hay muchas formas de modificar la visualización, entre otras por: el código de color de la entidad superior (cambios de color a medida que cambian los detalles del origen de datos), el filtro desde el gráfico de la visión de datos y las facetas de panel de control de investigación. La visión de datos se puede ver con cascos de realidad virtual.

    Para acceder a la visión de datos: en el panel de control de Investigación, pulse Añadir gráfico > gráfico de visión de datos.

IBM Security Guardium V10.1

- Infraestructura y plataforma:
  - Reforzamiento de plataforma con seguridad mejorada y mejoras en la accesibilidad y globalización
  - Soporte para dispositivos Guardium ejecutándose en un entorno Hyper-V. Hyper-V es una solución de virtualización de Microsoft.
- Mejoras en la gestión y soporte en el despliegue de Guardium:
  - Se ha mejorado la estabilidad y la fiabilidad de los agentes S-TAP y el análisis de la recopilación.
  - La vista de salud del Gestor central proporciona un panel de control centralizado para asesorar en el estado de los componentes de Guardium desplegados.
  - El proceso de vigilancia de S-TAP (guard_monitor) para UNIX/Linux y Windows es un proceso diseñado para supervisar la capacidad de respuesta y el rendimiento de S-TAP. Si la utilización de CPU de S-TAP supera el umbral configurado, o si S-TAP no responde a una solicitud de la consola, se pueden realizar las acciones siguientes:

        - Ejecutar guard_diag automáticamente.
        - Interrumpir automáticamente el proceso S-TAP.
        - Volcar el núcleo automáticamente e interrumpir el proceso S-TAP.
    - Las adaptaciones empresariales realizas hacen que los componentes de Guardium sean más fáciles de desplegar y utilizar en grandes entornos, entre otros:
        - Actualizaciones en el equilibrio de carga automático para mejorar la granularidad y el requilibrio de las solicitudes
        - Informes de alertas de progreso para trabajos de larga ejecución
        - Acceso más preciso de la consola de la interfaz de usuario (UI) para ayudar a los clientes a dividir los roles y acceder a Guardium
        - Configuraciones de plantilla y perfil para facilitar el despliegue y el control desde el Gestor central
        - Agregación selectiva para agilizar la creación de informes en grandes entornos
        - Soporte para tuplas de 7 elementos: Un grupo de tuplas permite combinar de forma conjunta distintos atributos para formar un único miembro de grupo compuesto. Ejemplo de grupo de tuplas de 7 elementos: IP cliente/Aplic fuente/Usuario BD/IP servidor/Nombre servicio/Usuario SO/nombre BD
    - Cobertura ampliada de orígenes de datos:
        - Mejoras en la sustitución por anomalías, cifrado y creación de informes desde el agente S-TAP en System i
        - Mejoras en el filtrado, encadenamiento de UID y usabilidad para agentes S-TAP para orígenes de datos z/OS
        - Funciones de seguridad de datos adicionales para más plataformas de Big Data: enmascaramiento de datos dinámicos para MongoDB, bloqueo para HortonWorks e integración con la plataforma de seguridad Ranger y Cassandra Kerberos
            - Integración de Ranger: Ranger ofrece una infraestructura de seguridad centralizada para gestionar el control de acceso más preciso sobre Hadoop y los componentes relacionados (Hive, HBase, HDFS, Yarn). Mediante la utilización de la consola de administración de Ranger, los usuarios pueden gestionar políticas relacionadas con el acceso a un recurso (archivo, carpeta, base de datos, tabla, columna, etc.) para un conjunto determinado de usuarios y/o grupos y aplicar las políticas en Hadoop. También pueden habilitar el seguimiento de auditorías y las analíticas de políticas para un control más profundo del entorno.
        - Soporte para el agente S-TAP RedHat 7.1 en la arquitectura Power 8 (big-endian y little-endian). Big-endian y little-endian se refiere al orden de los bytes, formando una palabra digital, en la memoria del sistema. Las palabras se pueden representar en formato big-endian o little-endian. El formato little-endian almacena el byte menos significativo en la dirección de memoria más baja con el byte más significativo almacenado en la dirección de memoria más alta.
        - Nuevo soporte para DB2 Analytics Accelerator para z/OS
        - Soporte de cifrado SSL y PostgreSQL 9.4
        - Con DB2 UDB y MS SQL, Guardium da soporte a count_big(*).
    - La integración de la seguridad que proporciona casos de uso sinérgicos para los problemas de seguridad difíciles en los silos de TI:
        - Protección frente a amenazas internas. Aprovecha la integración con IBM Security Privileged Identity Manager para descubrir amenazas internas.
        - Sistema de protección frente a amenazas. Trabajando conjuntamente con IBM Security QRadar e IBM Security XGS es posible detectar amenazas sin que lleguen al origen de datos impidiendo filtraciones de datos o la falta de alertas.
    - Vista previa de tecnología para herramientas adicionales de análisis de acceso a datos:
        - El Centro de investigación proporciona un lugar centralizado para ejecutar el seguimiento forense basado en los registros de auditoría.

IBM Security Guardium Vulnerability Assessment V10.1

- Reconocimiento de seguridad actualizado con el nuevo suceso de vulnerabilidad común (CVE) y otras pruebas de vulnerabilidades
- Infraestructura común compartida para el asesoramiento de vulnerabilidades desde la capa de aplicaciones hasta la infraestructura de fondo, con una integración con IBM Security AppScan

IBM Security Guardium for Files (FAM) V10.1

- Mejoras en la escalabilidad y el rendimiento para ayudar en el despliegue en grandes organizaciones
- Mejoras en el rendimiento de descubrimiento de FAM (File Activity Monitor)
- Soporte para el descubrimiento de FAM en AIX 6.1 y AIX 7.1 (sin clasificación). Soporte para el descubrimiento y la clasificación de unidades compartidas en el rastreador de FAM.

Tema principal: Visión general del producto

Notas del release

Conozca las últimas características y mejoras, los requisitos del sistema y la información de actualización, instalación y soporte.

Descripción de las mejoras y características nuevas

La versión más reciente de Guardium contiene muchas características nuevas y mejoras en la funcionalidad existente. Revise los enlaces siguientes para unas notas más detalladas del release:

- Notas de release de Guardium V10.1.4

- Notas de release de Guardium V10.1.3
- Notas de release de Guardium V10.1.2
- Notas de release de Guardium V10.1

Anuncio

Consulte el anuncio de publicación de IBM Guardium para obtener la siguiente información:

- Descripción detallada del producto, que incluye una descripción de la nueva funcionalidad
- Declaración de posicionamiento del producto
- Información de pedido y empaquetamiento
- Información de compatibilidad internacional

Requisitos del sistema

Para obtener información sobre las plataformas soportadas y los requisitos del sistema de Guardium V10.1, consulte http://www-01.ibm.com/support/docview.wss?uid=swg27047801.

Actualización de Guardium

Consulte Actualización del sistema Guardium para obtener información sobre cómo actualizar a la versión más reciente de Guardium.

Instalación de Guardium

Consulte Instalación del sistema Guardium para obtener información sobre cómo instalar la versión más reciente de Guardium.

Problemas conocidos

Los problemas conocidos se documentan y pasan a estar disponibles a través del sitio web de IBM Support.

A medida que se descubren y resuelven problemas, se actualiza el sitio web IBM Support. Busque en el sitio web de IBM Support para encontrar rápidamente métodos alternativos o soluciones a los problemas, así como otros documentos como, por ejemplo, requisitos detallados del sistema y descargas.

Ciclo de vida de soporte

Si está utilizando una versión anterior del software Guardium, planifique con antelación las actualizaciones. Puede encontrar información sobre fechas de fin de soporte para productos de IBM en el sitio web IBM Software Support Lifecycle.

Tema principal: Visión general del producto

Guía de inicio

- Guía de inicio a la interfaz de usuario
  Aprenda las funciones básicas de la interfaz de usuario de Guardium, incluido el inicio de sesión por primera vez, el banner y los menús de navegación, la interfaz de usuario y los datos de búsqueda.
- Personalización de la interfaz de usuario
  Guardium da soporte a la personalización del menú de navegación para usuarios y roles específicos.
- Inicio rápido para la supervisión y cumplimiento
  Aprenda a desplegar agentes de supervisión en los servidores de base de datos y a configurar la supervisión de bases de datos para que cumpla con los estándares y normas de seguridad.
- Vista de sistema
  La Vista de sistema es la vista inicial predeterminada para muchos usuarios. Permite ver elementos clave del estado del sistema.
- Supervisión de actividad de datos
  Información acerca de los conceptos clave de seguridad utilizados en la supervisión de la actividad de datos de Guardium.
- Supervisión de actividad de archivos
  La supervisión de actividad de archivos descubre los datos confidenciales en los servidores; clasifica el contenido utilizando definiciones predefinidas o definidas por el usuario; configura reglas y políticas acerca del acceso de datos y las acciones que se deben llevar a cabo cuando se cumplen las reglas.
- Conceptos clave y herramientas
  Información acerca de los conceptos clave que pertenecen a la administración de Guardium.

Información relacionada:
Visión general, arquitectura e interfaz de usuario de Guardium (vídeo)

Guía de inicio a la interfaz de usuario

Aprenda las funciones básicas de la interfaz de usuario de Guardium, incluido el inicio de sesión por primera vez, el banner y los menús de navegación, la interfaz de usuario y los datos de búsqueda.

Navegación

Al iniciar sesión por primera vez en la interfaz de usuario de Guardium, hay dos menús principales: el banner y el menú de navegación.

Puede expandir y colapsar el menú de navegación pulsando el icono de comillas angulares , o puede ocultar el menú de navegación por completo pulsando el icono mostrar / ocultar .

El diseño inicial de la pantalla está determinado por la licencia aplicada, el acceso permitido en función de los roles, el tipo de máquina y un factor de visibilidad. Ejemplos de roles son usuario, administrador, gestor de acceso y CLI. Los roles se asignan a los usuarios y aplicaciones para conceder privilegios de acceso específicos.

Navegadores web soportados

Internet Explorer 9 (IE9) y posterior en Windows 7. Aviso: al utilizar IE9 - (1) asegúrese de que el sitio web de su empresa no aparece en la selección Vista de compatibilidad de Internet Explorer; (2) Al exportar archivos, la descarga de archivos no esté bloqueada por la opción IE9 "No guardar las páginas cifradas en el disco". Cambie el valor de esta opción y exportar/descargar funcionará como se esperaba.

Firefox ESR 24 y posterior

Chrome 28 y posterior

Resolución de pantalla mínima - 1366 x 768

Menú de banner

El banner contiene los elementos siguientes:

Elemento	Descripción
Reloj de hora del sistema	La hora universal del sistema Guardium.
Lista de tareas pendientes	Contiene la Lista de tareas pendientes del proceso de auditoría, que se puede filtrar por usuario y los Procesos sin resultados pendientes.
Ayuda	Abra la ayuda del producto pulsando Ayuda > Ayuda de Guardium. Obtenga información acerca del sistema Guardium, como el número de versión, pulsando Ayuda > Acerca de Guardium. Para el contenido de ayuda específico de una pantalla o característica con la que está trabajando, pulse en el icono de ayuda pequeño que está incluido en el panel de la pantalla. Nota: Ambos iconos de ayuda le dirigen al mismo Information Center, en el que puede buscar y acceder a todo el contenido de la ayuda.
Búsqueda de interfaz de usuario / datos / archivos	Búsqueda de una parte de la interfaz, fragmentos de datos o un archivo. Por ejemplo, si desea buscar el Creador de políticas, conmute la búsqueda Interfaz de usuario, y escriba `creador de políticas`. Pulse cualquiera de los resultados para ir a la parte de la interfaz de usuario deseada.
Tipo de cuenta	Indica qué tipo de cuenta tiene. Edite los detalles de cuenta, por ejemplo el nombre o contraseña, personalice el diseño de la IU y cierre la sesión de Guardium de forma segura.
Tipo de máquina	Indica el tipo de máquina que está utilizando, por ejemplo autónoma, una unidad gestionada, un gestor central o un agregador.

El menú de banner también contiene mensajes de inicio importantes como, por ejemplo, poca memoria RAM, memoria de búsqueda rápida, requisito mínimo de CPU de 4 núcleos, caducidad del certificado, error en la gestión central, SSLv3 habilitado o inhabilitado, y no dispone de licencia.

Nota: Guardium recomienda que se inhabilite SSLv3. Sin embargo, al tratar con versiones antiguas de Guardium que no tienen instalada la última versión, si se inhabilita SSLv3, la funcionalidad de Gestión central se verá afectada entre el Gestor central y las unidades gestionadas.

Menú de navegación

Cada icono del menú de navegación representa una fase del ciclo de vida de seguridad de Guardium; pulse cualquier icono para expandirlo y ver los componentes de la fase. El menú de navegación centrado en el ciclo de vida es una forma de navegar por la interfaz de usuario y es coherente entre roles.Los elementos de menú se pueden personalizar y es posible que aparezca o no en función del rol.

Fase	Descripción
Configurar	Configure los valores de red, compruebe el estado de los servicios y configure las definiciones, grupos, alias y alertas de los orígenes de datos.
Gestionar	Gestione el estado general del entorno, S-TAP, datos, módulos, mantenimiento e informes.
Descubrir	Descubra automáticamente las bases de datos nuevas que se introducen en el entorno y busque y clasifique los datos confidenciales.
Reforzar	Asesore las debilidades actuales de su entorno con Asesoramiento de vulnerabilidades y supervise los cambios realizados en su entorno con CAS (Configuration Auditing System).
Investigar	Supervise las actividades de base de datos e investigue la actividad sospechosa en cualquier parte de su entorno.
Proteger	Proteja el entorno con las políticas de seguridad de datos que bloquean la actividad sospechosa e impida el acceso no autorizado a los datos. Para obtener más información acerca de las políticas, consulte Políticas.
Cumplir	Acceda a iniciativas de cumplimiento con procesos de auditoría y la creación de informes granular.

Informes	Cree su propio informe o utilice uno de los informes predefinidos para informar acerca de cualquier parte de su entorno. Para obtener más información acerca de los informes, consulte Informes.
Mis paneles de control	Cree sus propios paneles de control para revisar de forma sencilla los informes que le interesen. Para obtener más información acerca de los paneles de control, consulte Creación de paneles de instrumentos.

Iconos encontrados comúnmente

Muchas de las aplicaciones de creador y buscador en Guardium comparten este conjunto de iconos.

Icono	Descripción
Nuevo	Cree un elemento nuevo, por ejemplo un grupo o una definición de origen de datos.
Modificar	Modifique un elemento. Nota: Al modificar elementos, el método recomendado es clonar el elemento y, a continuado, modificar el clon.
Clonar	Clone un elemento para crear una copia.
Suprimir	Suprima un elemento.

Tema principal: Guía de inicio

Personalización de la interfaz de usuario

Guardium da soporte a la personalización del menú de navegación para usuarios y roles específicos.

Las herramientas Personalizar menú de navegación y Personalizar usuario/rol le permiten cambiar el contenido y la organización del menú de navegación. Puede acceder a dichas herramientas en varias ubicaciones:

- Todos los usuarios pueden personalizar su propio menú de navegación abriendo el menú Usuario en el banner Guardium y seleccionando Personalizar.
- Los usuarios administrativos pueden personalizar el menú de navegación para otros roles y usuarios abriendo el menú Usuario y seleccionando Personalizar usuario/rol o navegando a Configuración > Herramientas y vistas > Personalizar usuario/rol.
- Los usuarios que han iniciado sesión como *accessmgr* pueden personalizar el menú de navegación para otros roles y usuarios navegando a Acceso > Gestión de acceso, seleccionando Explorador de roles, y pulsando el enlace Personalizar menú de navegación.

La herramienta proporciona una experiencia de personalización coherente para todos los usuarios.

La lista Menú de navegación refleja la organización y contenidos del sistema de navegación de Guardium. Seleccione herramientas e informes de la lista Herramientas e informes disponibles y utilice el icono para añadir elementos a la lista Menú de navegación. Elimine elementos de la lista Menú de navegación pulsando el icono situado junto al elemento. Utilice los controles arrastrar y soltar o el icono para reorganizar elementos en la lista Menú de navegación.

Es posible definir una nueva página de inicio de Guardium (es decir, la primera página visible después de iniciar sesión en el sistema) seleccionando un elemento de la lista Menú de navegación y pulsando el icono .

Después de pulsar el botón Aceptar, el menú de navegación de Guardium se actualiza para reflejar los cambios que ha realizado en la lista Menú de navegación.

Se aplican las siguientes limitaciones cuando se utilizan estas herramientas:

- No puede suprimir el grupo Mis paneles de control, pero puede suprimir paneles de control individuales dentro del grupo.
- Los nuevos grupos vacíos no se guardarán.
- Los grupos vacíos mostrados en la lista Menú de navegación no aparecerán en el menú de navegación de Guardium.

Tema principal: Guía de inicio
Información relacionada:
Gestión de roles y permisos

Inicio rápido para la supervisión y cumplimiento

Aprenda a desplegar agentes de supervisión en los servidores de base de datos y a configurar la supervisión de bases de datos para que cumpla con los estándares y normas de seguridad.

Acerca de esta tarea

El inicio rápido para la supervisión y el cumplimiento está formado por las dos herramientas siguientes:

Desplegar agentes de supervisión

Utilice la herramienta Desplegar agentes de supervisión para activar automáticamente los clientes de GIM, instalar S-TAP y empezar a supervisar el tráfico de la base de datos.

La herramienta para desplegar agentes de supervisión simplifica el proceso de establecimiento de un despliegue de Guardium. En base a una infraestructura de Guardium Instalation Manager (GIM), la herramienta para desplegar agentes de supervisión le ayuda a buscar servidores de bases de datos, instalar agentes de supervisión (S-TAP) y configurar los motores de inspección para la base de datos.Además, la herramienta proporciona una vista centralizada para realizar un seguimiento y revisar el estado de despliegue.

Supervisión de cumplimiento

Después de desplegar agentes de supervisión (S-TAP), utilice la herramienta Supervisión del cumplimiento para establecer la supervisión de normativas y estándares de seguridad específicos.

Guardium proporciona varias plantillas de supervisión de cumplimiento: grupos, políticas de seguridad e informes correspondientes a regulaciones y estándares específicos, entre los que se incluyen los siguientes:

- Comité de Basilea sobre supervisión bancaria (BASEL II)
- Reglamento General de Protección de Datos (GDPR)
- Reglamento General de Protección de Datos (GDPR) para Db2 for z/OS (GDPR para Db2 for z/OS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Security Standard (PCI)
- Información de identificación personal (PII)
- Cumplimiento de Sarbanes-Oxley (SOX)

Estas plantillas de supervisión de cumplimiento de inicio rápido son especialmente útiles para las organizaciones que deben cumplir uno de las regulaciones o estándares asociados en un breve periodo de tiempo. Después de instalar las políticas de seguridad, la herramienta de supervisión de cumplimiento guía a los administradores o a los oficiales de cumplimiento por la configuración inicial y el relleno de grupos con información específica de la organización como, por ejemplo, direcciones IP de cliente e ID de usuarios privilegiados específicos. Además, la herramienta de supervisión de cumplimiento comprueba periódicamente el entorno de Guardium para ver si hay nuevas bases de datos que se puedan supervisar utilizando las plantillas de supervisión de cumplimiento.

Procedimiento

1. Revise la información siguiente para empezar a familiarizarse con las herramientas.
   - Inicio rápido para el despliegue de agentes de supervisión
   - Inicio rápido para la supervisión del cumplimiento
2. Desplegar agentes de supervisión para los servidores de bases de datos.
   a. Verifique que cumple con los requisitos previos para utilizar la herramienta para desplegar agentes de supervisión: Requisitos previos para desplegar agentes de supervisión.
   b. Desplegar agentes de supervisión en los servidores de bases de datos: Desplegar agentes de supervisión.
3. Configure la supervisión de cumplimiento para los servidores de base de datos.
   a. Verifique que cumple con los requisitos previos para utilizar la herramienta de supervisión de cumplimiento: Requisitos previos para la supervisión de cumplimiento
   b. Configure la supervisión de cumplimiento: Configurar supervisión del cumplimiento.
   c. Cumplimente grupos para identificar usuarios y aplicaciones que tienen permiso para acceder a las bases de datos: Rellenar grupos.
   d. Proporcione credenciales que permitan a Guardium acceder a las bases de datos para el descubrimiento y la clasificación de datos confidenciales: Habilitar el escaneo de datos confidenciales

Resultados

Después de desplegar correctamente los agentes de supervisión y configurar la supervisión de cumplimiento para los servidores de bases de datos, Guardium empieza a supervisar el tráfico de la base de datos.

Para obtener más información acerca de cómo interpretar lo que ve en la página de supervisión de cumplimiento, consulte Interpretación de las vistas de supervisión de cumplimiento.

Tema principal: Guía de inicio

Vista de sistema

La Vista de sistema es la vista inicial predeterminada para muchos usuarios. Permite ver elementos clave del estado del sistema.

Tres separadores bajo la vista del sistema muestran distintos tipos de información de estado:

- El Supervisor de estado de S-TAP muestra datos de resumen acerca de S-TAPs que se despliegan en su entorno. Los iconos representan el estado de alto nivel, y puede detallar más para ver más información acerca de los motores de inspección.
- El separador Utilización de unidad muestra información sobre el uso de cada sistema Guardium.
- El separador Supervisor del sistema muestra detalles actualizados acerca de los datos de entrada, el uso de la CPU y otra información.

Tema principal: Guía de inicio

Supervisión de actividad de datos

Información acerca de los conceptos clave de seguridad utilizados en la supervisión de la actividad de datos de Guardium.

- Políticas y reglas
  Una política de seguridad contiene un conjunto ordenado de reglas que se deben aplicar al tráfico observado entre servidores y clientes de base de datos. Cada regla se puede aplicar a una solicitud desde un cliente o a una respuesta desde un servidor. Se pueden definir e instalar varias políticas en un sistema Guardium al mismo tiempo.
- Flujos de trabajo
  Los flujos de trabajo consolidan varias tareas de supervisión de la actividad de la base de datos, incluidos el descubrimiento de activos, el asesoramiento y el

refuerzo de las vulnerabilidades, la supervisión de la actividad de la base de datos y la creación de informes de auditoría, la distribución de informes, la validación por parte de las partes interesadas y el escalamiento.

- Auditoría
  Guardium proporciona características de auditoría de cambios de valores para realizar el seguimiento de cambios en los valores de las tablas de base de datos.
- Clasificación
  Guardium da soporte al descubrimiento y la clasificación de datos confidenciales para permitir la creación y la aplicación de políticas de acceso eficaces.

Tema principal: Guía de inicio

Políticas y reglas

Una política de seguridad contiene un conjunto ordenado de reglas que se deben aplicar al tráfico observado entre servidores y clientes de base de datos. Cada regla se puede aplicar a una solicitud desde un cliente o a una respuesta desde un servidor. Se pueden definir e instalar varias políticas en un sistema Guardium al mismo tiempo.

Cada regla en una política define una acción condicional. La condición puede ser una simple prueba, por ejemplo una comprobación de cualquier acceso de una dirección IP de cliente no encontrada en un grupo de IP de cliente autorizado, o la condición puede ser una prueba compleja que evalúa varios atributos de mensaje y sesión, como un usuario de base de datos, programa de origen, tipo de mandato, hora del día, etc. Las reglas también pueden ser sensibles al número de veces que se cumple una condición dentro de un periodo de tiempo especificado.

La acción desencadenada por la regla puede ser una acción de notificación (por ejemplo, un correo electrónico a uno o más destinatarios, por ejemplo), una acción de bloqueo (desconexión de la sesión de cliente) o el suceso podría simplemente registrase como una infracción de política. Se pueden desarrollar acciones personalizadas para realizar las tareas necesarias para las condiciones que pueden ser únicas para una aplicación o entorno dado.

Tema principal: Supervisión de actividad de datos

Flujos de trabajo

Los flujos de trabajo consolidan varias tareas de supervisión de la actividad de la base de datos, incluidos el descubrimiento de activos, el asesoramiento y el refuerzo de las vulnerabilidades, la supervisión de la actividad de la base de datos y la creación de informes de auditoría, la distribución de informes, la validación por parte de las partes interesadas y el escalamiento.

Los flujos de trabajo están destinados a transformar la gestión de la seguridad de base de datos desde una actividad manual que requiere mucho tiempo y que se realiza periódicamente en un proceso automatizado que da soporte a los requisitos de privacidad y gobierno de empresa, como PCI-DSS. SOX, privacidad de datos e HIPAA. Además, los flujos de trabajo soportan la exportación de resultados de auditoría a repositorios externos para un análisis forense adicional a través de Syslog, archivos CSV/CEF y canales de información externos.

Por ejemplo, un proceso de automatización de flujo de trabajo de cumplimiento puede realizar las preguntas siguientes: qué tipo de informe, de asesoramiento, de seguimiento de auditoría o de clasificación se necesita, quién debería recibir esta información y como se manejan las validaciones, y cuál es la planificación de entrega.

Tema principal: Supervisión de actividad de datos

Auditoría

Guardium proporciona características de auditoría de cambios de valores para realizar el seguimiento de cambios en los valores de las tablas de base de datos.

Para cada tabla en la que se va a realizar un seguimiento de cambios, puede seleccionar qué mandatos de cambio de valor de SQL desea supervisar (insertar, actualizar, suprimir). Los valores anteriores y posteriores se capturan cada vez que se ejecuta un mandato de cambio de valor en una tabla supervisada. Esta actividad de cambio se carga en Guardium de forma planificada, tras la cual se pueden utilizar todas las funciones de informes y alertas de Guardium.

Puede ver datos de cambios de valores desde el informe Valores modificados predeterminado, o puede crear informes personalizados utilizando el dominio de Seguimiento de cambios de valores.

Tema principal: Supervisión de actividad de datos

Clasificación

Guardium da soporte al descubrimiento y la clasificación de datos confidenciales para permitir la creación y la aplicación de políticas de acceso eficaces.

Una política de clasificación es un conjunto de reglas diseñadas para descubrir y etiquetar elementos de datos confidenciales. Se pueden definir las acciones para cada regla en una política de clasificación, por ejemplo, para generar una alerta de correo electrónico o añadir un miembro a un grupo de Guardium, y las políticas de clasificación se pueden programar para que se ejecuten en los orígenes de datos especificados o como tareas de flujo de trabajo.

Las rutinas de descubrimiento y clasificación pasan a ser importantes a medida que el tamaño de una organización crece y la información confidencial como, por ejemplo, los números de tarjetas de crédito o los datos financieros personales se vuelven presentes en varias ubicaciones, a menudo sin el conocimiento de los administradores actuales responsables de los datos. Esto sucede con frecuencia en el contexto de las fusiones y las adquisiciones o cuando los sistemas existentes ya no son responsabilidad de los propietarios originales. La clasificación de Guardium descubre y etiqueta estos datos confidenciales para que se puedan aplicar las políticas de acceso.

Tema principal: Supervisión de actividad de datos

Supervisión de actividad de archivos

La supervisión de actividad de archivos descubre los datos confidenciales en los servidores; clasifica el contenido utilizando definiciones predefinidas o definidas por el usuario; configura reglas y políticas acerca del acceso de datos y las acciones que se deben llevar a cabo cuando se cumplen las reglas.

La supervisión de actividad consiste en las siguientes funcionalidades:

- El descubrimiento incluye la recopilación de metadatos y titularidades de archivos y carpetas.
- La clasificación utiliza *planes de decisiones* para identificar datos potencialmente sensibles en los archivos como, por ejemplo, la información de tarjetas de crédito o la información identificativa de individuos.

- La supervisión y recopilación de reglas de política y de información de auditoría, alertas en tiempo real o bloqueo de conexiones o usuarios sospechosos.

Supervisión de la actividad de archivos:

- Cumple con la conformidad con la normativa de un modo rentable
    - Automatiza y centraliza controles y proporciona seguimientos de auditoría.
    - Cumple con la conformidad con varias normativas como, por ejemplo, HIPAA, PCI DSS, diversas normativas de privacidad reconocidas internacionalmente.
- Escala con volúmenes de datos en crecimiento y con la expansión de los requisitos de empresa
- Proporciona un amplio soporte heterogéneo en muchos sistemas conocidos

Caso de uso 1

Los servidores de bases de datos o el acceso de fondo de las aplicaciones pueden acceder, modificar o incluso destruir archivos de aplicación críticos.

Solución: La supervisión de actividad de archivos puede descubrir y supervisar los archivos de configuración, archivos de registro, el código fuente y muchos otros archivos de aplicación críticos y alertar o bloquear cuando los procesos o usuarios no autorizados intenten acceder.

Caso de uso 2

Necesidad de proteger los archivos que contienen información de identificación personal (PII) o información de propiedad sin que ello afecte al negocio diario.

Solución: La supervisión de actividad de archivos puede descubrir y supervisar el acceso a los documentos confidenciales almacenados en muchos sistemas de archivos. Agregará los datos, proporcionará una vista de la actividad, avisará en caso de un acceso sospechoso y permitirá bloquear el acceso para seleccionar archivos, carpetas y usuarios.

Caso de uso 3

Necesidad de bloquear el acceso de fondo a los documentos gestionados por la aplicación.

Solución: La supervisión de actividad de archivos permite descubrir, supervisar y bloquear el acceso de fondo a los documentos, a los que normalmente se accede a través de un componente frontal de aplicación (por ejemplo, portal web).

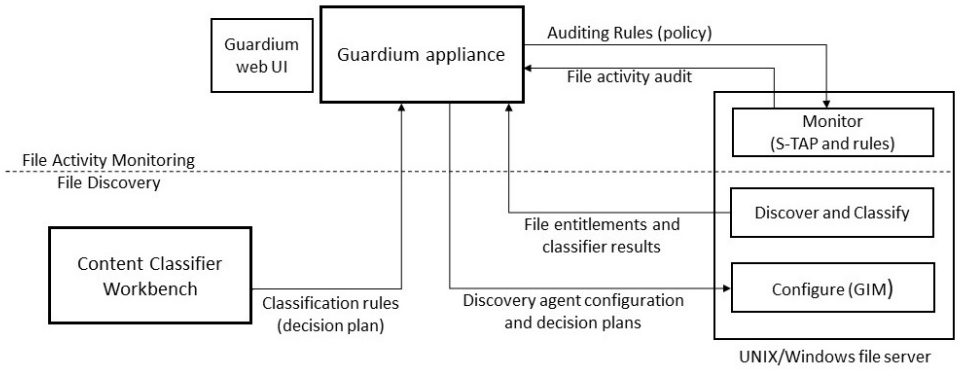
- Visión general y conceptos para la supervisión de actividad de archivos (FAM)
- Requisitos previos para la supervisión de actividad de archivos
- Flujo de trabajo de nivel superior para la supervisión de actividad de archivos
  Utilice este flujo de trabajo general para planificar y ejecutar la supervisión de la actividad de archivos.

Tema principal: Guía de inicio
Información relacionada:
Supervisión de la actividad de archivos utilizando Guardium (vídeo).

Visión general y conceptos para la supervisión de actividad de archivos (FAM)

La supervisión de la actividad de archivos (FAM) para servidores de archivos consta de las siguientes funcionalidades:

- El descubrimiento incluye la recopilación de metadatos y titularidades de archivos y carpetas.
- La clasificación utiliza *planes de decisiones* para identificar datos potencialmente sensibles en los archivos como, por ejemplo, la información de tarjetas de crédito o la información identificativa de individuos.
- La supervisión y recopilación de reglas de política y de información de auditoría, alertas en tiempo real o bloqueo de conexiones o usuarios sospechosos.



Descubrimiento y clasificación

El escaneo de **descubrimiento** básico identifica la lista de archivos y carpetas, su propietario, permisos de acceso, tamaño y la fecha y hora de la última actualización. También identifica los permisos de usuario y de grupo. El descubrimiento da soporte a todos los tipos de archivo. La **clasificación** se define mediante *planes de decisiones*. Cada plan de decisiones contiene reglas para reconocer un determinado tipo de datos. (Los planes de decisiones para la Supervisión de la actividad de los archivos son análogos a las políticas de clasificación para la supervisión de actividad de los datos). La clasificación incluye un gran número de tipos de archivos, entre los que se incluyen: texto sin formato, HTML, Office o PDF. Existen planes de decisiones predeterminados para el código fuente, HIPAA, PCI y SOX. Puede cambiar las entidades de clasificación desde los informes resultantes/Panel de control de investigación, utilizando los planes de decisiones predeterminados. Además, puede crear planes nuevos, o modificar planes existentes, utilizando Content Classifier Workbench, una aplicación Windows que se sube al dispositivo recopilador. Consulte en esta nota técnica de IBM los requisitos para IBM Content Classification Versión 8.8:http://www-01.ibm.com/support/docview.wss?uid=swg27020838. Los planes se activan y configuran a través de Guardium Installation Manager (GIM).

El descubrimiento y la clasificación son manejados por un agente de descubrimiento, denominado el rastreador de archivos. El rastreador de archivos envía los datos y los metadatos de archivo desde sus procesos de descubrimiento y clasificación al sistema Guardium. La planificación del escaneo es configurable. Los escaneos posteriores

(incrementales), después del descubrimiento y la clasificación iniciales, sólo identifican cambios incrementales de únicamente los archivos nuevos y modificados. Instale y configure el rastreador de archivos con GIM (Guardium Installation Manager) igual que lo haría con cualquier otro paquete.

Supervisión, auditoría y bloqueo

La supervisión de la actividad de los archivos se implementa mediante el S-TAP, que se ejecuta en el servidor de archivos. (La supervisión de actividad no requiere el paquete FAM que se utiliza con el descubrimiento y la clasificación). Para los volúmenes NFS, es importante tener un S-TAP instalado y configurado en todas las máquinas que acceden a dichos volúmenes. S-TAP gestiona la supervisión, las alertas y el bloqueo del acceso a los archivos, de acuerdo con las reglas de política de Guardium. Las reglas especifican los archivos y servidores de archivos a supervisar y qué acciones se deben tomar si se infringen las reglas de política, por ejemplo, registrar la infracción, alertar o bloquear el acceso. Las operaciones supervisadas son Leer, Escribir, Ejecutar, Suprimir, Cambiar propietario, Permisos, Propiedades. Cualquier actividad que coincide con los criterios de las reglas de política de seguridad se envía al recopilador Guardium donde se almacena en el repositorio Guardium. (En la supervisión de las actividades de base de datos, el S-TAP envía toda la actividad de datos a Guardium, donde se supervisa). Todos los sucesos registrados en el repositorio de Guardium son sucesos auditados.

Puesto que las reglas de supervisión de archivos se activan en el S-TAP, el bloqueo se produce de forma inmediata. Los datos solicitados por el usuario no se leen nunca desde el disco; el S-TAP bloquea e impide la operación. El acceso a los archivos también se puede bloquear, incluso si los permisos del sistema operativo permiten el acceso.

Las actividades de supervisión se presentan en los informes predefinidos: Privilegios de usuario, Privilegios de archivo, Recuento de actividad por usuario, Recuento de actividad por cliente, Archivos abiertos a "público", Usuarios latentes, Archivos latentes, etc., y el informe FAM - Acceso (registro de todas las actividades supervisadas) y en el Panel de control de investigación.

Importante: Las actividades de usuario Administrador de Windows y ROOT de Linux no se supervisan ni bloquean mediante la Supervisión de actividad de archivos (FAM).

Un agente S-TAP gestiona tanto la supervisión de la actividad de la base de datos como la del servidor de archivos. Si dispone de licencias para ambas funciones, puede utilizar el mismo agente S-TAP tanto para la supervisión de actividades de base de datos como de archivos. Instale y configure el S-TAP igual que lo haría con cualquier otro paquete.

Tema principal: Supervisión de actividad de archivos

Requisitos previos para la supervisión de actividad de archivos

Instale estos componentes para ejecutar la supervisión de actividad de archivos:

- Cliente GIM en todos los servidores de archivos
- S-TAP
- Claves de licencia
- Agente de descubrimiento de FAM (también conocido como el paquete FAM o agente FAM, que se necesita para el descubrimiento y la clasificación)
- Opcional: IBM Content Classification para los planes de decisiones no predeterminados http://www-01.ibm.com/support/docview.wss?uid=swg27020838

La supervisión de actividad de archivos da soporte a cadenas de UID: El agente FAM cambia el nombre de usuario individual por una cadena de nombres de usuario que pertenecen al historial del proceso (cadena de UID). Por ejemplo, si el Proceso 1 (usuario janedoe) crea el Proceso 2 (user johndoe), entonces para los sucesos de archivo relacionados con el proceso 2, FAM informa de la cadena de UID de {janedoe, johndoe}.

La supervisión de actividad de archivos no da soporte a:

- NAS (Network Attached Storage)

La supervisión de actividad de archivos da soporte a estos servidores:

Versión plataforma	Supervisión de FAM	Descubrimiento de FAM	Clasificación de FAM
aix-7.1-aix-powerpc	sí	sí	no
aix-6.1-aix-powerpc.	sí	sí	no
Red Hat 4 PowerPC	sí	no	no
Red Hat 5 S390X	sí	no	no
rhel-4-linux-i686	sí	no	no
rhel-4-linux-ia64	no	no	no
rhel-4-linux-x86_64	sí	no	no
rhel-5-linux-i686	sí	sí	sí
rhel-5-linux-ia64	no	no	no
rhel-5-linux-ppc64	sí	no	no
rhel-5-linux-x86_64	sí	sí	sí
rhel-6-linux-i686	sí	sí	sí
rhel-6-linux-ppc64	sí	no	no
rhel-6-linux-s390x	sí	no	no
rhel-6-linux-x86_64	sí	sí	sí
rhel-7-linux-x86_64	sí	sí	sí
suse-10-linux-i686	sí	sí	sí
SharePoint 2013	no	no	sí
suse-10-linux-ppc64	sí	no	no
suse-10-linux-s390x.	sí	no	no
suse-10-linux-x86_64	sí	sí	sí

Versión plataforma	Supervisión de FAM	Descubrimiento de FAM	Clasificación de FAM
suse-11-linux-i686	sí	sí	sí
suse-11-linux-s390x	sí	no	no
suse-11-linux-x86_64	sí	sí	sí
suse-12-linux-x86_64	sí	sí	no
Ubuntu 10 x86/64	sí	sí	no
Ubuntu 12 x86/64	sí	sí	sí
Ubuntu 14 x86/64	sí	sí	no
Windows 2008 Server	Sí	Sí	sí
Windows 2012 Server	Sí	Sí	sí

Tema principal: Supervisión de actividad de archivos

Flujo de trabajo de nivel superior para la supervisión de actividad de archivos

Utilice este flujo de trabajo general para planificar y ejecutar la supervisión de la actividad de archivos.

Flujo de trabajo de nivel superior para la supervisión de actividad de archivos

1. Instalación y activación de los componentes de supervisión de actividad de archivos en todos los servidores de archivos.
2. Descubrir y clasificar datos confidenciales en servidores de archivos.
3. Personalización de planes de decisiones de FAM opcional. Puede utilizar los planes de decisiones predeterminados o crear uno propio utilizando IBM Content Classification.
4. Supervisar y auditar
   - La actividad de archivos se puede incluir en los informes, incluidos los informes predefinidos siguientes. Informes predefinidos: privilegios de usuario, privilegios de archivo, recuento de actividad por usuario, recuento de actividad por cliente, archivos públicos, usuarios inactivos, archivos inactivos, etc.
   - Para los análisis e investigación en curso utilice los paneles de control de investigación, que incluyen la funcionalidad de búsqueda de texto y valores atípicos, además de visualizaciones mejoradas. Consulte:
     - Panel de control de investigación para archivos
     - Interpretación de los valores atípicos de actividad de archivos
5. Proteger: crear y aplicar políticas para la supervisión y protección en curso. Consulte Reglas y políticas de la actividad de archivos

- UNIX: El nivel de depuración se configura mediante tap_debug_output_level. Los registros de depuración y errores de FAM se denominan guard_stap.fam.txt. La ubicación predeterminada en UNIX es \tmp, y se configura mediante tap_log_dir
- Windows: El archivo del registro del agente de FAM se denomina StapAT.ctl y se ubica en la carpeta C:\Archivos de programa\IBM\Windows S-TAP\Logs.

Tema principal: Supervisión de actividad de archivos

Conceptos clave y herramientas

Información acerca de los conceptos clave que pertenecen a la administración de Guardium.

- Consulta e informes
  Las consultas de Guardium describen un conjunto de información que se debe obtener a partir de los datos recopilados. Los informes definen cómo se presentan los datos identificados por una consulta de Guardium.
- Control de acceso
  Guardium proporciona mapas de acceso como una forma de mostrar el acceso de datos entre los clientes de base de datos y los servidores de base de datos.
- Roles de usuario
  Un rol define un grupo de usuarios de Guardium que comparten los mismos privilegios de acceso.
- Grupos
  Guardium da soporte a la agrupación de elementos para simplificar la creación y la gestión de políticas y para agrupar la presentación de informes.
- Depuración y archivado de datos
  Archivado de datos realiza copias de seguridad de los datos que ha capturado el sistema Guardium. Al configurar Archivado de datos también pueden especificarse criterios de depuración de datos.
- Guardium Installation Manager
  Guardium Installation Manager (GIM) se utiliza para instalar y mantener los componentes de Guardium en los sistemas gestionados.

Tema principal: Guía de inicio

Consulta e informes

Las consultas de Guardium describen un conjunto de información que se debe obtener a partir de los datos recopilados. Los informes definen cómo se presentan los datos identificados por una consulta de Guardium.

Las consultas de Guardium describen un conjunto de información obtenida a partir de los datos recopilados. Las consultas están formadas por tres elementos: entidades, campos y condiciones. Las entidades definen el ámbito de una consulta, los campos listan las columnas de datos que la consulta debe devolver y las condiciones definen pruebas para que coincidan con los datos (mayor que, menos que, contiene, etc,)

Un informe define cómo se presentan los datos recopilados por una consulta. El informe predeterminado es un informe tabular que refleja la estructura de la consulta, con cada atributo visualizado en una columna distinta. Todos los parámetros de ejecución y componentes de presentación de un informe tabular se pueden personalizar.

Tema principal: Conceptos clave y herramientas

Control de acceso

Guardium proporciona mapas de acceso como una forma de mostrar el acceso de datos entre los clientes de base de datos y los servidores de base de datos.

El acceso de datos por parte de las aplicaciones y herramientas se puede clasificar de acuerdo a muchas dimensiones, incluidos los datos a los que se accede, la manera en la que se accede o el número de llamadas de SQL que se están realizando. En un entorno empresarial es muy importante obtener un buen control del acceso a la base de datos. Este requisito puede deberse a la necesidad de comprender y proteger el acceso a la base de datos debido a las iniciativas de conformidad e incluso a la necesidad de ajustar y optimizar el entorno de la base de datos. Puesto que puede haber muchas bases de datos y un número muy elevado de clientes de base de datos en entornos empresariales, obtener un control de las vías de acceso de datos puede ser una tarea difícil.

La topología de salud de despliegue y las vistas de tabla muestran las relaciones de flujo de datos entre los sistemas del entorno. Esta vista facilita la identificación de los sistemas problemáticos y la investigación de problemas subyacentes. Acceda a la vista de topología navegando a Gestionar > Vista de sistema > Topología de salud de despliegue. Acceda a la vista de tabla navegando a Gestionar > Vista de sistema > Tabla de salud de despliegue.

Tema principal: Conceptos clave y herramientas

Roles de usuario

Un rol define un grupo de usuarios de Guardium que comparten los mismos privilegios de acceso.

Cuando un rol se asigna a una aplicación o la definición de un elemento (una consulta específica, por ejemplo), solo pueden acceder a dicho componente aquellos usuarios de Guardium a los que también se les asigna ese rol. Si no se han asignado roles de seguridad a un componente (un informe, por ejemplo), solo el usuario que ha definido el componente y el usuario administrador pueden acceder al mismo.

En el momento de la instalación, Guardium se configura con un conjunto predeterminado de roles y de cuentas de usuario. El gestor de acceso de Guardium puede crear roles nuevos y modifica los roles existentes según sea necesario.

Tema principal: Conceptos clave y herramientas

Grupos

Guardium da soporte a la agrupación de elementos para simplificar la creación y la gestión de políticas y para agrupar la presentación de informes.

La agrupación puede simplificar el proceso de creación de definiciones de consulta y políticas. Agrupar elementos del mismo tipo puede ser útil, y la agrupación puede hacer que la presentación de la información sobre los informes sea más sencilla. Los grupos los utilizan todos los subsistemas y todos los usuarios comparten un único conjunto de grupos.

Para mostrar un ejemplo de agrupación, supondremos que su empresa tiene 25 objetos de datos separados que contienen información de empleados confidencial y que necesita realizar informes de todos los accesos a dichos elementos. Puede diseñar una prueba de consulta muy larga para cada uno de los 25 elementos. De forma alternativa, también puede definir un grupo único denominado información de empleados confidencial que contenga los 25 objetos. De esta forma, en las definiciones de consultas o reglas de política, solo es necesario probar si un objeto es miembro de dicho grupo.

Una ventaja adicional de los grupos es que se pueden facilitar los requisitos de mantenimiento cuando cambia la composición del grupo. Para continuar con el ejemplo, si la empresa decide que deben añadirse dos objetos más al grupo de información de empleados confidencial, solo necesita actualizar la definición del grupo, en lugar de todas las consultas, informes y políticas que hacen referencia al grupo.

Tema principal: Conceptos clave y herramientas

Depuración y archivado de datos

Archivado de datos realiza copias de seguridad de los datos que ha capturado el sistema Guardium. Al configurar Archivado de datos también pueden especificarse criterios de depuración de datos.

Hay dos operaciones de archivado: Archivado de datos y Archivado de resultados. La vía de acceso a estas operaciones es Gestionar > Gestión de datos > Archivado de datos o Archivado de resultados (Auditoría).

Archivado de datos
: Con Archivado de datos, los datos se archivan al final del día en el que se capturan, lo que garantiza que en el caso de una catástrofe, solo se perderán los datos de ese día. La depuración de los datos depende de la aplicación y de los requisitos empresariales y de auditoría, pero en la mayoría de los casos los datos se pueden mantener en las máquinas durante más de seis meses.

Archivado de resultados
: Archivado de resultados realiza una copia de seguridad de los resultados de las tareas de auditoría (p. ej. informes, pruebas de asesoramiento, seguimiento de auditoría de entidad, conjuntos de privacidad y procesos de clasificación), además de la vista de aprobación y los comentarios de los procesos de flujo de trabajo. Los conjuntos de resultados se depuran del sistema de acuerdo con la definición del proceso de flujo de trabajo.

En un entorno de agregación, los datos se pueden archivar desde el recopilador, el agregador o ambos. Más frecuentemente, los datos se archivan una sola vez y la ubicación en la que se archivan depende de los requisitos del cliente.

Tema principal: Conceptos clave y herramientas

Guardium Installation Manager

Guardium Installation Manager (GIM) se utiliza para instalar y mantener los componentes de Guardium en los sistemas gestionados.

El componente GIM incluye un servidor de GIM, que se instala como parte del sistema Guardium, y un cliente de GIM, que debe instalarse en los servidores que alojan las bases de datos y los servidores de archivos que desea supervisar. Después de instalar el cliente de GIM, este funciona con el servidor de GIM para realizar las tareas siguientes:

- Comprobar si hay actualizaciones del software instalado
- Transferir e instalar software nuevo
- Desinstalar software
- Actualizar parámetros de software

Si el entorno incluye un sistema Guardium configurado como un gestor central, debe decidir qué sistemas Guardium desea utilizar como servidores de GIM. Puede gestionar todos los clientes de GIM desde un único sistema Guardium como, por ejemplo, el gestor central, o bien puede gestionarlos en grupos desde los distintos sistemas Guardium. Si gestiona todos los clientes de GIM desde un único sistema Guardium puede ver el estado de todos los clientes de GIM y realizar tareas relacionadas desde una única interfaz. Si opta por gestionar los clientes de GIM en grupos de sistemas Guardium distintos, puede utilizar cada sistema para gestionar los clientes GIM que gestionar, pero no hay disponible ninguna vista general o de entorno.

Tema principal: Conceptos clave y herramientas

Descubrir

Descubrir hace referencia a los procesos de localización e identificación de objetos en su entorno que deben rastrearse con fines de seguridad y cumplimiento.

Descubrir es el proceso de encontrar objetos importantes como usuarios privilegiados, datos confidenciales y orígenes de datos. Clasificación es el proceso de identificar de forma apropiada lo que se ha descubierto por motivos de seguridad y cumplimiento. Estos procesos de descubrir y clasificación son importantes en grandes organizaciones donde las fusiones, adquisiciones y sistemas existentes introducen nuevos objetos en su entorno de forma no estructurada e imprevisible. Guardium le ayuda a incorporar estos objetos en su entorno para que pueda aplicar políticas de seguridad efectivas y garantizar el cumplimiento.

Un escenario común implica el descubrimiento de datos confidenciales. Los datos confidenciales hacen referencia a información regulada como, por ejemplo, los números de tarjeta de crédito, datos financieros personales, números de la seguridad social y otra información que requiere una gestión especial. Guardium soporta dos aproximaciones diferentes para descubrir datos confidenciales: Utilizando el creador de flujos de trabajo Descubrir datos confidenciales, o utilizando el creador de políticas con otras herramientas de Guardium. El creador de flujos de trabajo Descubrir datos confidenciales está pensado como una herramienta completa para establecer procesos de descubrimiento y clasificación para datos confidenciales. Utilícelo para especificar reglas para el descubrimiento, definir acciones a realizar en los datos descubiertos, especificar qué orígenes de datos escanear, distribuir informes y ejecutar el flujo de trabajo en una planificación automática. Para usuarios más avanzados, el Constructor de políticas admite reglas de descubrimiento y clasificación más granulares que se pueden incorporar fácilmente a las aplicaciones de Guardium.

- Orígenes de datos
  Los orígenes de datos almacenan información sobre la base de datos o el repositorio como, por ejemplo, el tipo de base de datos, la ubicación del repositorio o las credenciales que se pueden asociar con el mismo. Debe definir un origen de datos para poder utilizarlo con las aplicaciones de Guardium.
- Protección del servicio de base de datos en la nube
  La protección del servicio de base de datos en la nube proporciona clasificación, asesoramiento de vulnerabilidades y auditoría de objetos en bases de datos en la nube.
- Descubrimiento automático de base de datos
  La aplicación de descubrimiento automático escanea y sondea sus servidores en busca de puertos abiertos para impedir las conexiones no deseadas o desconocidas a su red. Puede ejecutar procesos de descubrimiento automático a petición o planificar el proceso de forma periódica.
- Clasificación
  Los procesos y políticas de clasificación definen cómo Guardium descubre y trata los datos confidenciales como, por ejemplo, los números de tarjetas de crédito, números de la seguridad social y datos financieros personales.
- Descubrir datos confidenciales
  Cree un escenario integral para descubrir y clasificar datos confidenciales.
- Expresiones regulares
  Se pueden utilizar expresiones regulares para buscar tráfico de patrones complejos en los datos.
- Descubrir y clasificar datos confidenciales en servidores de archivos
  La supervisión de la actividad de archivos garantiza la integridad y la protección de los datos confidenciales en servidores de archivos UNIX y Windows.
- Optimización de titularidades
  La Optimización de titularidades media entre el rol del administrador de base de datos, para proporcionar a los usuarios las titularidades necesarias para realizar sus trabajos de forma eficiente y, el rol de seguridad para mantener las titularidades tan precisas y mínimas como sea posible para evitar vulnerabilidades del sistema.

Orígenes de datos

Los orígenes de datos almacenan información sobre la base de datos o el repositorio como, por ejemplo, el tipo de base de datos, la ubicación del repositorio o las credenciales que se pueden asociar con el mismo. Debe definir un origen de datos para poder utilizarlo con las aplicaciones de Guardium.

- Creación de una definición de origen de datos
  Utilice el Creador de orígenes de datos para crear definiciones de orígenes de datos para utilizarlas con las aplicaciones de Guardium.
- Cómo trabajar con orígenes de datos existentes
  Después de crear una definición de origen de datos, puede clonar el origen de datos, modificarlo o suprimirlo.
- Informes sobre orígenes de datos
  Guardium proporciona informes sobre los orígenes de datos de su entorno y cualquier cambio realizado en ellos.
- Definición de un origen de datos utilizando un nombre de servicio
  Puede definir un origen de datos que permita a sus usuarios conectarse con una base de datos Oracle utilizando el nombre de servicio mediante un URL personalizado.
- Gestión de definiciones de KDC
  Si su origen de datos requiere autenticación mediante Kerberos, puede especificar la información necesaria para Guardium para obtener un tíquet de Kerberos antes de realizar la conexión.

Tema principal: Descubrir

Creación de una definición de origen de datos

Utilice el Creador de orígenes de datos para crear definiciones de orígenes de datos para utilizarlas con las aplicaciones de Guardium.

Acerca de esta tarea

Puede crear una definición de origen de datos mediante dos procesos generales. En primer lugar, puede añadir una definición de origen de datos desde el Creador de orígenes de datos y, a continuación, especificar la aplicación para la que desea utilizar el origen de datos. En segundo lugar, puede ir a la aplicación que desea utilizar y crear un origen de datos dentro de la aplicación. La navegación para añadir una definición de origen de datos en una aplicación específica varía según la aplicación que

elija o el tipo de base de datos seleccionado. Por ejemplo, si desea crear una base de datos de auditoría, navegue a Reforzar > Control de cambios de configuración (Aplicación CAS) > Creación de base de datos de auditoría de cambio de valores y pulse Añadir origen de datos.

Procedimiento

- Abra el Creador de orígenes de datos navegando a Configurar > Definiciones de orígenes de datos.
- Pulse para añadir una definición de origen de datos.
- Utilice el diálogo Crear origen de datos para proporcionar información sobre el origen de datos a almacenar para su uso futuro. Dependiendo de la aplicación, el tipo de base de datos que seleccione y el tipo de origen de datos que utilice, el diálogo varía ligeramente.
  1. Seleccione un Tipo de aplicación.
  2. Especifique un Nombre exclusivo para el origen de datos.
  3. Desde el menú Tipo de base de datos, seleccione la base de datos o tipo de archivo. Para algunas aplicaciones, el origen de datos debe ser una base de datos y no puede ser un archivo de texto. En función del tipo de base de datos que seleccione, algunos campos del panel estarán inhabilitados o cambiarán las etiquetas. Por ejemplo, Asignar credenciales puede ser opcional u obligatorio. Cuando es obligatorio, está inhabilitado y los campos de nombre de usuario y contraseña son obligatorios. Cuando es opcional, el nombre de usuario y la contraseña se inhabilitan hasta que se selecciona Asignar credenciales.
  4. Seleccione Compartir origen de datos para compartir la definición de origen de datos en todas las aplicaciones. Si no comparte el origen de datos, la definición que ha creado solo se puede utilizar con la aplicación que elija.
  5. Opcionalmente, configure credenciales adicionales.
     - Utilizar SSL: Seleccione para utilizar SSL. A continuación, seleccione, opcionalmente, Importar certificado SSL de servidor y pulse Añadir certificado para seleccionar el certificado.
     - Utilizar LDAP: Seleccione para utilizar LDAP. A continuación, pulse Asignar credenciales y especifique el nombre de usuario y la contraseña
     - Utilizar Kerberos: Seleccione para utilizar una configuración Kerberos predefinida. Seleccione una Configuración de Kerberos y especifique el Reino y KDC. El origen de datos lo compara con sus propios KDC y Reino para asegurarse de que coinciden.
  6. Seleccione Guardar contraseña para guardar y cifrar sus credenciales de autenticación en el dispositivo de Guardium. Es necesario guardar la contraseña si está definiendo un origen de datos con una aplicación que se ejecuta como tarea planificada (opuesto a petición). Cuando se selecciona guardar contraseña, el nombre de inicio de sesión y la contraseña son necesarios.
  7. Especifique sus credenciales para Nombre de inicio de sesión y Contraseña.
  8. Para el campo IP/Nombre de host, especifique el nombre de host o la dirección IP para el origen de datos.
  9. Utilice la tabla para completar el Puerto en función de su tipo de origen de datos.

     Tabla de tipo de origen de datos y número de puerto

Tipo de base de datos	**Número de puerto**
Aster Data	2046
DB2	50000 Con DB2 UDB, Guardium da soporte a count_big(*). En tablas muy grandes, un count(*) estándar podría fallar.
DB2 for i	446
DB2 for z/OS	446
GreenplumDB	5432
Hadoop	21000-21050
Informix	1526

Tipo de base de datos	Número de puerto
MS SQL Server (Puertos dinámicos) y MS SQL Server (DataDirect: Puertos dinámicos)	Número de puerto en gris: El uso de este origen de datos permite a un cliente sin un valor de puerto definido o donde la función dinámica está habilitada desde el servidor de bases de datos MS SQL Server conectar dinámicamente con una base de datos del servidor de MS SQL. Para definir el puerto dinámico, vaya al servidor de BD de MS SQL Server y defina 0 en el tipo de puerto dinámico y elimine el puerto TCP/IP que, de forma predeterminada, es el puerto 1433. Establecer el valor del puerto dinámico en 0 y reiniciar los servicios establecerá una IP dinámica. Con MS SQL, Guardium da soporte a count_big(*). En tablas muy grandes, un count(*) estándar podría fallar. Controlador DataDirect para MS SQL Server Anteriormente, el controlador jTDS tenía que descargarse para poder dar soporte a la autenticación de Windows utilizando NTLM y NTLMv. Ahora el controlador DataDirect de Guardium lo permitirá. Parámetros Si el usuario de Guardium desea utilizar la autenticación de Windows, añada este parámetro a la Propiedad de conexión: domain=domain_name;AuthenticationMethod=ntlmjava Si utiliza NTLMv2 para la autenticación de Windows, añada este parámetro a la Propiedad de conexión: domain=domain_name;AuthenticationMethod=ntlm2java AuthenticationMethod Finalidad Determina que método de autenticación utiliza el controlador al establecer una conexión. Si el método de autenticación especificado no está soportado por el servidor de bases de datos, la conexión falla y el controlador emite una excepción. Valores válidos auto | kerberos | ntlm | ntlmjava | ntlm2java | userIdPassword Notas Si especifica AuthenticationMethod=ntlmjava cuando LMCompatabilityLevel se ha restringido a NTLMv2, devolverá un error. Cuando LMCompatabilityLevel se ha restringido a NTLMv2, AuthenticationMethod debe establecerse en ntlm2java. Si especifica AuthenticationMethod=ntlmjava o AuthenticationMethod=ntlm2java, debe especificar el nombre y el servidor de dominio que administra la base de datos. Puede especificar el servidor de dominio utilizando la propiedad Domain. Si no se especifica la propiedad Domain, el controlador intenta determinar el servidor de dominio desde las propiedades de usuario. Si el controlador no puede determinar el nombre del servidor de dominio, emite una excepción. La propiedad User proporciona el ID de usuario. La propiedad Password proporciona la contraseña. Los valores type4, type2 y none están en desuso, pero se reconocen por razones de compatibilidad con versiones anteriores. Utilice en su lugar los valores kerberos, ntlm y userIdPassword, respectivamente. La autenticación NTLM requiere Microsoft SQL Server 2000, Service Pack 3 o superior. Si el usuario Guardium está utilizando Unicode de base de datos no estándar como Azeri_Cyrillic_100_CI_AS o Chinese_Hong_Kong_Stroke_90_CI_AS, añada este parámetro a la propiedad de conexión: CodePageOverride=UTF-8 Si utiliza SSL (Force encryption=Yes), añada: encryptionMethod=SSL;validateServerCertificate=false
MS SQL Server (DataDirect)	1433
MongoDB	27017
MySQL	3306
Netezza	5480
Oracle (DataDirect)	1521
PostgreSQL	5432
Sybase	4100

Tipo de base de datos	Número de puerto
Sybase IQ	2638
Teradata	1025
Texto	0
Texto:HTTP	8000
Texto:FTP	21
Texto:SAMBA	445
Texto:HTTPS	8443
N_D	0
MS SQL Server (código abierto) (utilice Reforzar > Asesoramiento de vulnerabilidades > Subidas de cliente para subir estos controladores JDBC, consulte Subida de grupos suscritos).	1433
Oracle (código abierto) (utilice Reforzar > Asesoramiento de vulnerabilidades > Subidas de cliente para subir estos controladores JDBC, consulte Subida de grupos suscritos).	1521
HIVE, HiveServer2	10000
HADOOP, CLI Hive en desuso	9083
HIVE, para Impala desde Hue	21050
HADOOP, Shell de Impala	21000
HUE, programa de fondo de Hue Oracle	1521
HUE, programa de fondo de Hue MySQL	3306
HUE, programa de fondo de Hue PostgreSQL	5432
WEBHDFS	50070

Nota: Cuando se intenta conectar utilizando un origen de datos SSL por primera vez, es posible que se produzca este error al probar la conexión:

```
error
Connection unsuccessful
Could not connect to: 'jdbc:db2://su11u1x64t-va:55000/VA_DB' for user: '(DELETE ME) db2 10.1 SSL_DB2(Security
Assessment)'. DataSourceConnectException: Could not connect to: 'DB2 (DELETE ME) db2 10.1 SSL 9.70.146.39:55000' for
user: 'db2inst1'. Exception: com.ibm.db2.jcc.am.DisconnectNonTransientConnectionException: [jcc][t4][2030][11211]
[4.15.134] A communication error occurred during operations on the connection's underlying socket, socket input stream,
```

Esto es debido a que la GUI no tiene el archivo de almacén de claves correcto para el certificado cargado en la memoria. Para corregirlo, reinicie la GUI y este error debería desaparecer y la conexión debería ser correcta.

10. En función del tipo de origen de datos, el diálogo varía ligeramente para los campos después del puerto.
    - Si es DB2, especifique el nombre de la base de datos.
    - Si es DB2 iSeries u Oracle, especifique el nombre de servicio.
    - Si es Informix, especifique el nombre del servidor de Informix.
    - Para un tipo de base de datos que no sea de texto, en el recuadro de Base de datos, especifique el nombre de la base de datos (Solo Informix, Sybase, MS SQL Server, PostgreSQL o Teradata). Si está en blanco para Sybase o MS SQL Server, el valor predeterminado es maestro. Para base de datos Sybase, el recuadro de texto de base de datos debe contener el nombre de base de datos o el valor predeterminado, maestro, si está en blanco (Funciona para Informes de titularidad y clasificador. Para el asesoramiento de vulnerabilidades utilice el nombre de instancia de base de datos).
    - Para DB2, DB2 iSeries u Oracle especifique un nombre de esquema válido en el recuadro Esquema a utilizar.
    - Para un tipo de base de datos de archivo de texto, en el recuadro Nombre de archivo, especifique el nombre del archivo.
11. Utilice el recuadro Propiedad de conexión solo si se deben incluir propiedades de conexión adicionales en el URL de JDBC para establecer una conexión JDBC con este origen de datos. El formato necesario es propiedad=valor, donde cada pareja de propiedad valor está separada de la siguiente por una coma.
    - Para una base de datos Sybase con un conjunto de caracteres predeterminados de Roman8, especifique la siguiente propiedad: charSet=utf8.
    - Para una conexión cifrada de Oracle debe definir una propiedad de conexión como: oracle.net.encryption_client=REQUIRED;oracle.net.encryption_types_client=RC4_40 (Reemplazando con un algoritmo de cifrado necesario para la instancia supervisada, independientemente de su tipo).
    - Tenga en cuenta que el cifrado 3DES168 es problemático. Un origen de datos definido para utilizar el cifrado 3DES168 lanzará incorrectamente un error de protocolo ORA-17401 o un error de sumas de comprobación ORA-17002 cuando se encuentra cualquier error SQL. A partir de entonces, la conexión simplemente no funcionará hasta que se cierre y se vuelva a abrir.
    - Para una conexión cifrada de DB2 debe definir una propiedad de conexión como: securityMechanism=13.
    - Para una conexión DB2 iSeries defina una propiedad de conexión como: property1=com.ibm.as400.access.AS400JDBCDriver;translate binary=true
    - Para origen de datos DB2 z/OS, añada una propiedad de conexión para mejorar el rendimiento de la base de datos: resultSetHoldability=2
    - En Oracle, sys es un usuario predeterminado de Oracle, es el propietario de la instancia de base de datos y tiene privilegios de superusuario, como el root en Unix. SYSDBA es un rol y tiene privilegios administrativos necesarios para realizar muchas operaciones administrativas de alto nivel como iniciar y detener la base de datos así como realizar operaciones como la copia de seguridad y la recuperación. Este rol (SYSDBA) también puede otorgarse a otros usuarios. La frase `sys as SYSDBA` hace referencia al método necesario para conectarse como usuario sys.
    - Para valores de supervisor para Oracle 10 (sys as SYSDBA) (este es para el controlador de código abierto de Oracle), especifique lo siguiente: internal_logon=sysdba
    - Para DataDirect (controlador Oracle), especifique lo siguiente: SysLoginRole=sysdba
    - Además, si utiliza CRYPTO_CHECKSUM_TYPES en su sqlnet.ora, utilice los siguientes ejemplos:
    - oracle.net.encryption_client=aes256;oracle.net.crypto_checksum_types_client=SHA1
    - oracle.net.encryption_client=rc4_256;oracle.net.crypto_checksum_types_client=MD5
    - oracle.net.encryption_client=aes256;oracle.net.crypto_checksum_types_client=MD5
    - oracle.net.encryption_client=rc4_256;oracle.net.crypto_checksum_types_client=SHA1

- Ejemplo: Utilice la autenticación para LDAP de Oracle conocida como OID. Los valores necesarios son: El host de servidor o IP de LDAP, el puerto del servidor LDAP, el nombre de instancia de Oracle y el reino. El URL personalizado debe estar especificado correctamente: jdbc:guardium:oracle:@ldap://wi3ku2x32t4:389/on0maver,cn=OracleContext,dc=vguardium,dc=com

12. Si es necesario, especifique una serie de conexión de URL personalizado al origen de datos. Cuando el campo URL personalizado está en blanco, la conexión se realiza utilizando las propiedades especificadas en los otros campos de definición de origen de datos (por ejemplo, host, puerto, instancia, etc.).
    Importante:
    - Al especificar un campo de URL personalizado con el formato Oracle Open Source, especifique `jdbc:guardium:oracle://;SID=<SID>`.
    - Al crear un origen de datos para una base de datos Oracle con la seguridad avanzada de Oracle habilitada, especifique `EncryptionLevel=required` en el campo URL personalizado de la definición del origen de datos.
    -
13. Pulse Mostrar opciones avanzadas para visualizar las opciones Roles y CAS.
14. Opcionalmente, pulse Roles para asignar roles a los orígenes de datos. La adición de un rol a un origen de datos permitirá a los usuarios ver la configuración del origen de datos. Solo los propietarios y los administradores tienen permiso para modificar y suprimir el origen de datos.
15. Opcionalmente, especifique la información de CAS

    a. Puesto que los proveedores ofrecen flexibilidad durante la instalación, se debe preguntar a los usuarios para ayudarles a determinar los dos campos necesarios en la definición de origen de datos.

    CAS necesita dos partes de información: Una cuenta de instancia de base de datos para ejecutar alguna de las herramientas de base de datos en Unix y el nombre del directorio de la instancia de base de datos para encontrar los archivos a supervisar. Generalmente, si la cuenta de instancia de base de datos y el directorio no se han especificado correctamente en la definición de origen de datos, verá mensajes de `No hay datos CAS disponibles` para las pruebas en las que CAS no ha podido encontrar los datos.

    Especifique una Cuenta de instancia de base de datos (propietario de software) y un Directorio de instancia de base de datos (directorio donde se instaló el software de la base de datos) que utilizará CAS.

    Estas son sugerencias sobre cómo encontrar la información necesaria para cumplimentar la información CAS para los orígenes de datos. Esta información puede variar de una instalación a otra. Una de las formas utilizadas en Unix es listar el archivo /etc/passwd para instalaciones específicas de bases de datos que se pueden utilizar para identificar la cuenta de instancia de base de datos y el directorio. A veces, durante la instalación, se define una variable de entorno en la cuenta de instancia de base de datos que identifica el directorio de la instancia, por ejemplo, ORACLE_HOME. En este caso, especifique $ORACLE_HOME en el campo directorio de instancia de base de datos en el formulario de la definición del origen de datos y la variable se ampliará para encontrar el nombre de directorio correcto en el servidor de bases de datos.
    Nota: Para buscar varios directorios, puede definir varias vías de acceso de archivo para el Directorio de instancia de base de datos. Consulte la fila MongoDB para ver un ejemplo.

Tabla 1. Instancias de base de datos

Tipo de base de datos	**Cuenta de instancia de base de datos**	**Directorio de instancia de base de datos/Sugerencias adicionales**
DB2	Con frecuencia db2inst1	Directorio de inicio de db2inst1 o C:\Program Files\IBM\SQLLIB en Windows. El programa db2cmd.exe debe estar en la vía de acceso del sistema o en el subdirectorio bin del directorio de instancia de base de datos.
Informix	Con frecuencia informix	Algo parecido a /opt/IBM/informix en Unix o C:\Program Files\IBM\Informix. Se puede definir una variable de entorno INFORMIXDIR. El programa <servicename>.cmd debe estar en la vía de acceso del sistema donde <servicename> es el valor especificado en el servidor Informix de la definición de origen de datos.
MongoDB	Con frecuencia mongodb o mongos	Con MongoDB, debe especificar varias vías de acceso para el directorio de instancia de base de datos. Indique una vía de acceso separada utilizando una barra vertical "|" con espacios. Por ejemplo, /var/lib/mongo | MongoBinary=/usr/bin | dbpath=/var/lib/mongo | logpath=/var/log/mongodb | keytab=/home/keytab | dbdumppath=/opt/backup | sslpath=/etc/ssl | keyfile=/home/mongod/mongo_server.keyfile. La vía de acceso /var/lib/mongo es necesaria, puesto que es la vía de acceso inicial para el usuario mongo. MongoBinary=/usr/bin es la vía de acceso al binario de mongo. Debe especificar la variable (sensible a las mayúsculas y minúsculas) y, a continuación, igual a la vía de acceso. dbpath=/var/lib/mongo es la vía de acceso a los archivos de datos. En este caso, resulta ser la misma que el directorio de inicio de MongoDB. logpath=/var/log/mongodb es la vía de acceso al registro de MongoDB. keytab=/home/keytab es el directorio del archivo de tabla de claves de MongoDB. dbdumppath=/opt/backup es el directorio del núcleo de copia de seguridad de MongoDB. sslpath=/etc/ssl es la vía de acceso a los archivos SSL de MongoDB. keyfile=/home/mongod/mongo_server.keyfile apunta al archivo de claves de MongoDB. No es necesario que defina todas las vías de acceso listadas. Las vías de acceso no definidas no se analizarán.

Tipo de base de datos	Cuenta de instancia de base de datos	Directorio de instancia de base de datos/Sugerencias adicionales
Oracle	Con frecuencia oracle, o específico de versión como oracle9 u oracle10.	Por ejemplo, /home/oracle9 en Unix, o C:\oracle\product\10.2.0\db_1 en Windows. Se puede definir una variable de entorno ORACLE_HOME. En Windows, se deben definir las variables de entorno PERL5LIB y ORACLE_HOME y el programa opatch.bat debe estar en la vía de acceso del sistema.
SQL Server	No es necesario a menos que se esté utilizando la autenticación de Windows. En ese caso, debe estar en el formato aceptable para la autenticación de Windows, DOMAIN/Username.	Hay dos escenarios al cumplimentar el Directorio de instancia de base de datos para el uso de CAS en SQL Server. Si el origen de datos está siendo utilizado para pruebas de asesoramiento de vulnerabilidades, esta columna debe cumplimentarse con el directorio de inicio de instancia de base de datos. Ejemplos MSSQL2000, Instancia de nombre en un servidor de 64 bits. C:\Program Files (x86)\Microsoft SQL Server\MSSQL$MSSQL2000 MSSQL2000, instancia predeterminada en un servidor de 32 bits. C:\Program Files\Microsoft SQL Server\MSSQL MSSQL2005 C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL MSSQL2008 C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL Si el origen de datos no está siendo utilizado para pruebas de asesoramiento de vulnerabilidades, sino para archivos de supervisión o registro de CAS. Entonces esta columna será el directorio de Microsoft SQL Server con Program Files. Ejemplos C:\Program Files (x86)\Microsoft SQL Server o C:\Program Files\Microsoft SQL Server Nota: Debe tener dos orígenes de datos si desea realizar pruebas de asesoramiento de vulnerabilidades y supervisión de archivos CAS.
Sybase	Con frecuencia "sybase"	Para Unix /home/sybase, o C:\sybase para Windows. Se puede definir una variable de entorno SYBASE.
MySQL		Se puede definir una variable de entorno MYSQL_HOME. Nota: No está soportado un origen de datos MySQL con un nombre de base de datos Unicode. El nombre del origen de datos en MYSQL debe ser ASCII.
Teradata		No es necesario. Todas las instalaciones tienen el mismo aspecto.
Netezza		No es necesario. La instalación se encuentra en la misma ubicación en todas las máquinas.
PostgreSQL		Esta es la instalación más flexible. Es necesario que el usuario defina dos variables de entorno en el servidor de bases de datos de Postgres: PostgreSQL_BIN debe ser la ubicación de los binarios de la instalación y PostgreSQL_DATA la ubicación de los datos.

Nota: Si se va a utilizar una variable de entorno en el campo Directorio de instancia de base de datos, esa variable debe definirse en el servidor de bases de datos.

b. Seleccione una Clasificación de gravedad (o nivel de impacto) para el origen de datos. La clasificación de gravedad se puede utilizar para ordenar, filtrar o centrarse orígenes de datos mientras está viendo informes y resultados.
c. Pulse Guardar para guardar la definición de origen de datos (no puede añadir roles o comentarios hasta que la definición se ha guardado).
d. Opcionalmente, pulse Añadir comentarios para añadir comentarios a la definición.
e. Opcionalmente, pulse Probar conexión para probar la conectividad de los orígenes de datos definidos.
f. Pulse Cerrar cuando haya acabado con la definición.

Tema principal: Orígenes de datos

Cómo trabajar con orígenes de datos existentes

Después de crear una definición de origen de datos, puede clonar el origen de datos, modificarlo o suprimirlo.

Procedimiento

- Abra el Creador de orígenes de datos navegando a Configurar > Definiciones de orígenes de datos.
- El menú Selección de aplicaciones lista todas las aplicaciones con las que puede utilizar una definición de origen de datos. Elija la aplicación para la que se ha creado el origen de datos que desea modificar y pulse Siguiente esto le llevará al Buscador de orígenes de datos.

Tema principal: Orígenes de datos

Clonación de un origen de datos

Procedimiento

- Seleccione el origen de datos que desea clonar en el Buscador de orígenes de datos y pulse Clonar.
- La información que especificó cuándo creó la definición de origen de datos aparece en el diálogo Definición de origen de datos, con "Copia de" antes del nombre original del origen de datos. Cambie los campos que desee.
- Pulse Aplicar para guardar el origen de datos clonado.

Modificación de un origen de datos

Procedimiento

- Seleccione el origen de datos que desea modificar en el Buscador de orígenes de datos y pulse Modificar.
- La información que especificó cuándo creó la definición de origen de datos aparece en el diálogo Definición de origen de datos. Cambie los campos que desee.
- Pulse Aplicar para guardar los cambios realizados en el origen de datos.

Eliminación de un origen de datos

Procedimiento

Seleccione el origen de datos que desea modificar en el Buscador de orígenes de datos y pulse Suprimir.

Informes sobre orígenes de datos

Guardium proporciona informes sobre los orígenes de datos de su entorno y cualquier cambio realizado en ellos.

Procedimiento

- Abra el informe Orígenes de datos navegando a Informes > Herramientas de configuración de informes > Orígenes de datos. La tabla que aparece lista todos los orígenes de datos y la información almacenada en cada definición de origen de datos.
- Pulse el botón derecho del ratón sobre cualquier celda de la tabla y verá dos opciones: Historial de la versión de origen de datos e Invocar.
  - Pulse Historial de la versión de origen de datos para ver los cambios realizados en la definición de origen de datos.
  - Pulse Invocar para seleccionar y ejecutar una de las API disponibles para el origen de datos.

  Nota: Puede personalizar el tiempo de ejecución y los parámetros de presentación del informe de orígenes de datos pulsando el icono del lápiz.

Tema principal: Orígenes de datos
Conceptos relacionados:
Funciones de orígenes de datos de GuardAPI

Definición de un origen de datos utilizando un nombre de servicio

Puede definir un origen de datos que permita a sus usuarios conectarse con una base de datos Oracle utilizando el nombre de servicio mediante un URL personalizado.

Acerca de esta tarea

Debe especificar el nombre de host, el puerto y el nombre de servicio así como el URL personalizado.

Procedimiento

1. Determine el nombre de servicio Oracle. Puede utilizar mandatos como estos:

   ```
   SQL> set line size 5000;
   SQL> select host_name, instance_name from v$instance;
   SQL> select name from v$database;
   SQL> show parameter service
   ```

   Utilice el nombre que aparece en la columna VALOR.
2. Cargue el controlador ligero JDBC de Oracle adecuado en el sistema Guardium.
   a. Busque y baje el controlador para su base de datos Oracle aquí: http://www.oracle.com/technetwork/database/enterprise-edition/jdbc-112010-090769.html
   b. Abra la ventana Subidas de cliente navegando a Reforzar > Asesoramiento de vulnerabilidades > Subidas de cliente.
   c. Localice la sección titulada Subir controlador JDBC de Oracle. Pulse Examinar y navegue hasta la ubicación donde ha descargado el archivo. Pulse Utilizar un controlador de código abierto para todo.
   d. Reinicie la interfaz de usuario de Guardium una vez finalizada la subida.
3. Defina el origen de datos para esta base de datos.
   a. Abra el Creador de orígenes de datos navegando a Configurar > Definiciones de orígenes de datos.
   b. El menú Selección de aplicaciones lista todas las aplicaciones con las que puede utilizar una definición de origen de datos. Elija la aplicación para la que se ha creado el origen de datos que desea modificar y pulse Siguiente esto le llevará al Buscador de orígenes de datos.
   c. Especifique el nombre de servicio en el campo Nombre de servicio. En el campo URL personalizado, especifique `jdbc:oracle:thin@//hostname:port/svcname` donde hostname y port son los valores predeterminados para la base de datos y svcname es el nombre del servicio, el mismo valor que especificó en el campo Nombre de servicio.

Tema principal: Orígenes de datos

Gestión de definiciones de KDC

Si su origen de datos requiere autenticación mediante Kerberos, puede especificar la información necesaria para Guardium para obtener un tíquet de Kerberos antes de realizar la conexión.

Acerca de esta tarea

Desde Guardium V. 10.1.3 puede asignar un KDC a un origen de datos específico o un grupo de unidades gestionadas, para proporcionar una autenticación Guardium para bases de datos Mongo e Hive. El dispositivo obtiene un tíquet a través de la conexión JDBC, para que los usuarios no necesiten obtener tíquets ellos mismos. Tenga en cuenta que esto es independiente de la configuración propia del dispositivo.

Puede definir hasta 5 Key Distribution Centers (KDC) de Kerberos en un Gestor central y uno en un Guardium autónomo. Para añadir un Key Distribution Center a Guardium especifique:

- reino: Nombre del dominio en letras mayúsculas
- KDC: Nombre de host del servidor Kerberos
- tipo de cifrado para los tíquets de Kerberos
  - des-cbc-md5
  - des-cbc-crc
  - rc4-hmac
  - des3-cbc-sha1
  - aes128-cts-hmac-sha1-96
  - aes256-cts-hmac-sha1-96

  El valor predeterminado es aes256-cts-hmac-sha1-96, que es el tipo de cifrado más seguro.

Procedimiento

1. Pulse Configuración > Herramientas y vistas > Configuración de Kerberos
2. Pulse para crear una nueva configuración.
3. Especifique el Nombre, KDC y Reino.
4. Especifique el Tipo de cifrado. El valor predeterminado es aes256-cts-hmac-sha1-96.
5. Pulse Guardar.

Qué hacer a continuación

Después de haber creado un KDC de Kerberos, puede seleccionarlo cuando configure su configuración de origen de datos.

Tema principal: Orígenes de datos

Protección del servicio de base de datos en la nube

La protección del servicio de base de datos en la nube proporciona clasificación, asesoramiento de vulnerabilidades y auditoría de objetos en bases de datos en la nube.

Una vez que haya configurado la conexión de Guardium con la nube, puede:

- Descubrir instancias de bases de datos y catalogarlas en Guardium.
- Asignar orígenes de datos catalogados a un proceso de clasificación o crear un nuevo proceso: La clasificación se ejecuta en las bases de datos en la nube e identifica los objetos según las reglas definidas.
- Asignar orígenes de datos catalogados en un proceso de asesoramiento de vulnerabilidades o crear un nuevo proceso (requiere una licencia válida de asesoramiento de vulnerabilidades): El asesoramiento de vulnerabilidades se ejecuta en las bases de datos en la nube y utiliza los datos en los informes de Guardium.
- Habilitar la auditoría de BD: Los datos de auditoría estándar de Oracle se extraen de la nube para los informes de Guardium, en función de las políticas instaladas. (Consulte las definiciones de Oracle en: https://docs.oracle.com/cd/B28359_01/server.111/b28337/tdpsg_auditing.htm#TDPSG50051)
- Habilitar la auditoría de objetos (seguimiento de auditoría de Oracle). Revisar los resultados de la clasificación y seleccionar objetos para la auditoría de objetos. (La auditoría de base de datos debe estar habilitada). La auditoría de objetos realiza el seguimiento de todas las actividades realizadas en los objetos. Guardium utiliza estos datos para los informes, el panel de control de investigación, etc. Puede configurar Guardium para añadir objetos automáticamente, por origen de datos. También puede establecer un valor predeterminado para cuenta, que heredan todos sus orígenes de datos. Esto es realmente útil para las bases de datos cuyos objetos necesitan auditoría sin ninguna evaluación adicional. Debería establecer un límite alto pero razonable para lo que espera que encuentre el proceso de clasificación. Para evitar un desbordamiento de objetos, si hay un error en su clasificación, no establezca un valor demasiado alto. (Un desbordamiento podría afectar al rendimiento de la base de datos).

Se necesitan permisos de AWS para realizar las funciones de Guardium en la BD en la nube. Consulte Definición de IAM de AWS.

En bases de datos locales, el S-TAP instalado en la base de datos envía todo el tráfico de base de datos al sistema Guardium. En el entorno de nube, Guardium extrae archivos de registro de la base de datos en la nube y procesa los datos similares a los datos S-TAP. La diferencia es que el S-TAP registra toda la actividad de la base de datos, mientras que en el entorno de nube, solo se auditan las tablas que ha seleccionado. Otra diferencia es que puede haber una ligera demora en la recuperación de datos de la nube.

La actividad en las bases de datos y objetos auditados se escribe en los registros de base de datos. El volumen de la actividad registrada aumenta con el número de elementos supervisados. Las actividades de registro de gran volumen pueden afectar al rendimiento de la base de datos. Debe asegurarse de que se están capturando todos los datos relevantes y que el sistema no se sobrecarga.

Puede ejecutar la protección del servicio de bases de datos en la nube en un entorno de gestor central y en un recopilador Guardium autónomo.

En el contexto de la protección del servicio de bases de datos en la nube, la base de datos hace referencia a la base de datos en la nube y el origen de datos hace referencia a la base de datos catalogada de Guardium.

Solo un sistema Guardium puede poseer la auditoría de BD y de objeto de cualquier base de datos. Otros sistemas Guardium pueden acceder a la misma cuenta en la nube y ver los detalles de la base de datos, pero no pueden inhabilitar la auditoría de BD o acceder a los datos de auditoría de objetos. Puede traspasar la propiedad de un sistema de Guardium a otro, por ejemplo si uno deja de funcionar sin la expectativa de poder recuperarlo.

Se da soporte al descubrimiento, a la clasificación y al asesoramiento de vulnerabilidades (VA) en todos los motores de base de datos AWS RDS.

Limitaciones en la auditoría de base de datos

- Es necesario mantener actualizada la definición de RDS, por ejemplo, supresiones de instancias de BD o cambios en las credenciales.
- Guardium v10.1.4 solo da soporte a bases de datos Oracle V.11 en una nube AWS.
- No se da soporte a las reglas de extrusión, ni a la redacción y la realización de pruebas de patrones en los datos devueltos.
- No se da soporte a los datos devueltos, incluidos los registros afectados y el registro de valores de variables vinculadas.
- No se da soporte a las acciones de regla que interactúan con S-TAP; por ejemplo, S-GATE Terminate, Ignorar y Reescribir consultas.
- La auditoría nativa de Oracle no captura inicios de sesión fallidos y, por lo tanto, no es posible enviarlos a Guardium.
- Sentencias que la auditoría nativa de Oracle no ha capturado, por ejemplo, sentencias con errores de sintaxis no se pueden supervisar.

- Flujo de trabajo de protección del servicio de base de datos en la nube
- Definición de IAM de AWS
  Definir su política de IAM para su cuenta de AWS de acuerdo a sus permisos.
- Crear, modificar, suprimir cuentas en la nube
  Crear una cuenta de servicio de base de datos en la nube con sus credenciales de base de datos, modificar o suprimir la cuenta en la nube.
- Descubrir bases de datos en la nube
  Descubrir bases de datos en la cuenta en la nube seleccionando las regiones en las que desea buscar.
- Catalogar y gestionar bases de datos
  Catalogar bases de datos para crear los orígenes de datos en Guardium, modificar usuarios y contraseñas y actualizar la configuración de la base de datos.
- Gestionar el asesoramiento de vulnerabilidades y la clasificación
  Asignar orígenes de datos a un proceso de clasificación o de asesoramiento de vulnerabilidades, o crear nuevos procesos.
- Configurar la auditoría de bases de datos
  Habilitar la auditoría en la base de datos para que los datos de auditoría de objetos los pueda extraer Guardium. Modificar el límite de objetos añadidos automáticamente a la clasificación y modificar el recopilador.
- Gestionar auditoría de objetos
  Visualizar los objetos potencialmente confidenciales identificados por los procesos de clasificación en las bases de datos que gestiona y habilitar la auditoría de objetos en los objetos seleccionados para supervisar todas las actividades realizadas en esos objetos.

Tema principal: Descubrir

Flujo de trabajo de protección del servicio de base de datos en la nube

Acerca de esta tarea

Este es un flujo de trabajo general. Su flujo de trabajo específico depende de lo que desee conseguir con la auditoría de bases de datos en la nube.

Procedimiento

1. Cree una cuenta en la nube.
2. Descubra sus instancias de base de datos.
3. Catalogue las bases de datos con las que desea trabajar. La catalogación crea un origen de datos en Guardium, para que pueda gestionar las funciones de Guardium de base de datos en la nube en la base de datos específica.
4. Opcionalmente, añada el origen de datos a un proceso de asesoramiento de vulnerabilidades nuevo o existente (requiere licencia de asesoramiento de vulnerabilidades).
5. Opcionalmente, añada el origen de datos a un proceso de clasificación nuevo o existente.
6. Opcionalmente, habilite la auditoría de BD en las bases de datos relevantes y reinícielas desde la interfaz de usuario de Guardium ahora o desde la consola de BD más adelante. Una vez que la auditoría de BD está habilitada, esta realiza la auditoría de Oracle estándar. Cuando habilita una auditoría de base de datos, su sistema Guardium se vuelve el propietario exclusivo de la auditoría de base de datos en esta base de datos. Ningún otro sistema Guardium puede modificar la auditoría de base de datos o de objeto. Para ver los resultados de la clasificación, ejecute una vez la clasificación (Ejecutar una vez ahora) después de habilitar la auditoría de BD o espere a la siguiente ejecución planificada. (Debe asignarse el origen de datos a un proceso de clasificación).
7. Revise los resultados de la clasificación de sus orígenes de datos (requiere un proceso de clasificación y una auditoría de BD):
   - Vea los objetos, agrupados por objeto o por el proceso de clasificación que los ha identificado, utilice filtros para refinar los resultados.
   - Habilite o inhabilite la auditoría de objetos: Individualmente, por tabla.
   - Descienda desde la agrupación de objetos para abrir una lista con todas las bases de datos que contienen el objeto seleccionado en sus resultados de clasificación. En esta vista también puede habilitar e inhabilitar la auditoría de objetos.
8. Repita periódicamente los pasos 2 a 7.
9. Revise periódicamente los orígenes, buscando objetos nuevos y, opcionalmente, añadiendo o eliminando objetos de la auditoría de objetos. Por ejemplo, puede eliminar objetos si los objetos añadidos automáticamente incluyen objetos que ha decidido que no necesitan de auditoría o si una base de datos está teniendo problemas de rendimiento. O puede identificar un objeto sospechoso que no se ha auditado y añadirlo a la auditoría de objetos.

Tema principal: Protección del servicio de base de datos en la nube

Definición de IAM de AWS

Definir su política de IAM para su cuenta de AWS de acuerdo a sus permisos.

Los permisos de IAM mínimos incluyen ver la configuración y cambiar códigos. No incluyen la habilitación de la auditoría de BD, o el reinicio de una BD. Este JSON define los permisos mínimos, sin los que no es posible ejecutar la protección del servicio de base de datos en la nube.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "rds:DescribeDBParameters",
                "rds:DescribeDBInstances",
                "rds:DescribeDBParameterGroups",
                "rds:DownloadDBLogFilePortion",
                "rds:DescribeDBLogFiles",
                "rds:ListTagsForResource",
                "rds:RemoveTagsFromResource",
```

```
                "rds:AddTagsToResource",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcs"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Los permisos completos se habilitan con estos parámetros.

Habilitar, inhabilitar auditoría de BD en la instancia
: Cuando no se ha configurado, los botones Habilitar auditoría de base de datos e Inhabilitar auditoría de base de datos aparecen inactivos y debe solicitar al DBA habilitar o inhabilitar la instancia de BD en la consola de AWS.

```
"rds:CopyDBParameterGroup",
"rds:CreateDBParameterGroup",
"rds:ModifyDBInstance",
"rds:ModifyDBParameterGroup",
```

Reiniciar la instancia de BD
: Cuando no está configurada, los botones de Reiniciar están inactivos, deberá solicitar al DBA reiniciar la instancia de BD en la consola de AWS.

```
"rds:RebootDBInstance",
```

Manejar un grupo de seguridad cuando la plataforma soportada es EC2
: Cuando no está configurada, el DBA debe añadir la dirección IP de Guardium al grupo de seguridad. Cuando está configurada, Guardium añade su dirección IP al grupo de seguridad de la instancia de BD. Si el sistema de Guardium no puede identificar su propia dirección IP debido a la configuración de la red, el DBA debe añadir la dirección IP a la consola de AWS.

```
 "rds:ModifyDBInstance"
"rds:AuthorizeDBSecurityGroupIngress",
"rds:CreateDBSecurityGroup",
```

Manejar un grupo de seguridad cuando la plataforma soportada es VPC
: Cuando no está configurada, el DBA debe añadir la dirección IP de Guardium al grupo de seguridad. Cuando está configurada, Guardium añade su dirección IP al grupo de seguridad de la instancia de BD. Si el sistema de Guardium no puede identificar su propia dirección IP debido a la configuración de la red, el DBA debe añadir la dirección IP a la consola de AWS.

```
 "rds:ModifyDBInstance"
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CreateSecurityGroup",
```

Al configurar estos parámetros, Guardium crea una regla de entrada en el grupo de seguridad de instancia de RDS, con la máscara de CIDR de IP pública de recopilador = 24.

Tema principal: Protección del servicio de base de datos en la nube

Crear, modificar, suprimir cuentas en la nube

Crear una cuenta de servicio de base de datos en la nube con sus credenciales de base de datos, modificar o suprimir la cuenta en la nube.

Tema principal: Protección del servicio de base de datos en la nube

Crear una cuenta en la nube

Acerca de esta tarea

Requisito previo: Definir la política IAM de AWS. Consulte Definición de IAM de AWS para obtener más información.

Consejo: Si está gestionando un gran número de bases de datos en esta cuenta, considere definir un proceso de clasificación predeterminado. Esto le ahorra tener que definir las propiedades para cada base de datos descubierta.

Procedimiento

1. Navegue a Descubrir > Descubrimiento de base de datos > Protección de servicios de base de datos en la nube.
2. Pulse para abrir el panel Crear definición de cuenta de servicio de base de datos en la nube.
3. Defina la cuenta.
   - Nombre exclusivo de la cuenta
   - Proveedor
   - ID de clave de acceso único e ID de clave de acceso secreto tal como los proporciona el proveedor de sus servicios en la nube. La clave secreta de cuenta funciona como una contraseña. Tanto la clave de acceso y como el título deben ser exclusivos para que no existan varios nombres de cuenta con el mismo acces_id.
   - Limitar objetos añadidos automáticamente (opcional): Este es el número máximo de objetos encontrados por clasificación que pueden habilitarse automáticamente para la auditoría de objetos, cuando la auditoría de base de datos está habilitada. Puede modificarlo, por base de datos, después de ser descubiertas. Los objetos que se habilitan automáticamente aparecen como Habilitado en la ventana de objetos gestionados. Si desea que Guardium añada objetos automáticamente, establezca un límite alto pero razonable de lo que espera que encuentre el proceso de clasificación. Para evitar un desbordamiento de objetos si hay un error en su clasificación, no establezca un valor demasiado alto. (Un desbordamiento podría afectar al rendimiento de la base de datos). Cero (0) significa que no se habilitarán objetos automáticamente para la auditoría de objetos. Si el número de objetos auditados más el número de objetos acabados de clasificar supera este límite, no se habilitan nuevos objetos para la auditoría de objetos. Por ejemplo, si lo establece en 15 y la clasificación identifica 5 objetos la primera vez que se ejecuta, se asignan 5 objetos al seguimiento de auditoría. Si se establece en 15 y hay 5 objetos ya habilitados para la auditoría de objetos y la próxima ejecución de clasificación identifica 16 objetos, no se habilita ningún objeto para la auditoría de objeto. Si se establece en 15 y hay 5 objetos ya habilitados para la auditoría de objetos y la próxima ejecución de clasificación identifica 5 objetos, los 5 nuevos objetos se habilitan para la auditoría de objetos.

4. Opcionalmente, defina la clasificación predeterminada. Todas las bases de datos catalogadas en esta cuenta se asignan a este proceso de clasificación. Puede modificar el proceso de clasificación, por base de datos, después de ser catalogadas.
5. Pruebe el acceso a la nube.
    a. Pulse Probar acceso. Guardium intenta acceder a la nube.
    b. Si Guardium no puede acceder a la nube: Compruebe que su sistema Guardium tiene acceso a Amazon; compruebe las claves que ha proporcionado.
6. Pulse Crear.
   Se crea la cuenta y la lista de Cuentas de servicios de base de datos en la nube se actualiza con la nueva cuenta en la nube, con sus detalles de cuenta en el panel derecho.

Qué hacer a continuación

Descubrir bases de datos y catalogarlas, configurar la clasificación y el asesoramiento de vulnerabilidades y auditoría de objetos.

Modificar una cuenta en la nube

Todos los parámetros, excepto el proveedor, pueden modificarse.

Procedimiento

1. Seleccione la cuenta en la nube en Cuentas de servicios de base de datos en la nube y pulse en el panel derecho.
2. Modifique la configuración.
3. Si se han modificado algunas credenciales, pruebe el acceso a la nube pulsando Probar acceso.
4. Pulse Guardar.

Suprimir una cuenta en la nube

Suprimir una cuenta en la nube inhabilita la auditoría de objetos y de base de datos en todas las bases de datos propiedad del entorno actual.

Procedimiento

1. Seleccione la cuenta en el panel Cuentas de servicios de base de datos en la nube, pulse y confirme.
2. Reinicie la base de datos desde la consola de base de datos. Si no tiene acceso de Amazon a la base de datos, pida a su administrador de base de datos que inhabilite la auditoría de base de datos y que reinicie la base de datos. Es importante detener la auditoría y reiniciar la base de datos para que la base de datos detenga la escritura en los archivos de registro utilizados por Guardium.

Descubrir bases de datos en la nube

Descubrir bases de datos en la cuenta en la nube seleccionando las regiones en las que desea buscar.

Acerca de esta tarea

La tabla de bases de datos se cumplimenta y actualiza cuando ejecuta Descubrir. Una vez que se ha descubierto una base de datos, permanece en la tabla, independientemente de si la base de datos sigue en la nube.

Cada vez que navega a Descubrimiento > Descubrimiento de base de datos > Protección de servicios de base de datos en la nube, Guardium le informa de si el estado de la auditoría de base de datos en la nube es diferente del estado informado en la interfaz de usuario, con un mensaje sobre la tabla de base de datos: `El estado de auditoría de base de datos ha cambiado para algunas bases de datos. Pulse Actualizar para actualizar la tabla`. Cuando vea este mensaje, pulse Renovar para renovar la pantalla.

También puede realizar esta comprobación a petición pulsando Recuperar estado. La recuperación puede tardar unos minutos. Cuando se completa, únicamente aparece un mensaje si alguno de los estados de auditoría ha cambiado. Si hay cambios, pulse Renovar.

También puede subir definiciones de base de datos en la nube con un archivo CSV. Se muestra una lista de los parámetros necesarios en Funciones de orígenes de datos de GuardAPI Cloud; el parámetro de API cloudTitle se debe sustituir con el parámetro environmentTitle (tienen la misma función, pero nombres diferentes). Consulte el procedimiento de subida en Crear origen de datos para CSV subido mediante el menú Subir CSV en Subidas de cliente, utilizando la vía Reforzar > Asesoramiento de vulnerabilidades > Subidas de cliente para subir su archivo.

Procedimiento

1. Navegue a Descubrimiento > Descubrimiento de base de datos > Protección de servicios de base de datos en la nube y pulse el nombre de cuenta de servicio.
   Cuando crea una cuenta en la nube, la tabla Descubrir bases de datos está abierta, mostrando una lista de todas las regiones con sus puntos finales de RDS.
2. Cuando accede a esta página posteriormente, la tabla está cerrada. Pulse Descubrir bases de datos. Se abre la tabla mostrando las regiones.
3. Seleccione la fila de cada región cuyas bases de datos desee descubrir. Utilice el filtro si es necesario.
4. Pulse Descubrir. Guardium busca las regiones y añade cualquier base de datos que no haya sido descubierta antes a la tabla de bases de datos.

Tema principal: Protección del servicio de base de datos en la nube

Catalogar y gestionar bases de datos

Catalogar bases de datos para crear los orígenes de datos en Guardium, modificar usuarios y contraseñas y actualizar la configuración de la base de datos.

Acerca de esta tarea

La catalogación crea orígenes de datos dentro de Guardium que se utilizan para la clasificación, asesoramiento de vulnerabilidades, auditorías e informes. Las bases de datos no catalogadas tienen un icono rojo en la columna de origen de datos de Guardium de la tabla de BD.

Procedimiento

1. Catalogue las bases de datos que desea auditar.
    a. En la tabla Bases de datos, seleccione una o más bases de datos.
    b. Pulse Origen de datos > Origen de datos de catálogo.
    c. Especifique el usuario y contraseña de base de datos sensible a las mayúsculas y minúsculas que le proporcionó su administrador de base de datos. Si ha seleccionado más de una base de datos, asegúrese que desea utilizar el mismo par de usuario y contraseña para las mismas.
    d. Opcionalmente, modifique o borre el proceso de clasificación predeterminado.
    e. Pulse Catálogo.

   El nombre de origen de datos de Guardium aparece en la tabla de bases de datos.
2. Actualice el usuario o la contraseña:
    a. En la tabla Bases de datos, seleccione una o más orígenes de datos.
    b. Pulse Origen de datos > Actualizar usuario y contraseña y modifique los detalles. Se deben especificar ambos campos.
    c. Pulse Catálogo.
3. Modifique una definición de origen de datos.
    a. Seleccione el origen de datos y pulse Origen de datos > Abrir definición de origen de datos
    b. Modifique como sea necesario. Consulte los detalles de parámetros en Creación de una definición de origen de datos.
    c. Opcionalmente, pruebe la conectividad con la base de datos pulsando Probar conexión.
    d. Pulse Guardar.

Tema principal: Protección del servicio de base de datos en la nube

Gestionar el asesoramiento de vulnerabilidades y la clasificación

Asignar orígenes de datos a un proceso de clasificación o de asesoramiento de vulnerabilidades, o crear nuevos procesos.

Acerca de esta tarea

El menú Asesoramiento de vulnerabilidades solo está disponible si tiene una licencia de VA válida.

Una vez que asigne un proceso de clasificación a un origen de datos, los datos de clasificación se recopilan y gestionan igual que una base de datos local. Puede asignar una clasificación cuando no es el propietario, pero debe poseer la propiedad para habilitar la auditoría de objetos y la visualización de los resultados.

Un icono verde indica que el proceso se está ejecutando. Un icono amarillo significa que no hay definida una planificación para el proceso. Un icono rojo en la columna de Proceso de clasificación o VA indica que no se ha asignado una clasificación o VA, o que hay un error. Visualice errores de VA en Reforzar > Asesoramiento de vulnerabilidades > Creador de asesoramientos > Ver resultados. Visualice errores de clasificación en Descubrir > Escenarios integrales > Descubrir datos confidenciales > cinta Revisar informes > Registro de procesos.

Si le aparece un error de clasificación `file bdump-file-listing in BDUMP not found Unable to retrieve results for: 'RDSADMIN.TRACEFILE_` añada `RDSADMIN` al grupo de esquemas predefinidos `Esquemas de clasificación excluidos - Oracle` en el Creador de grupos.

Procedimiento

1. Asigne uno o más orígenes de datos a un proceso de clasificación existente.
    a. Seleccione uno o más orígenes de datos.
    b. Pulse Clasificación > Añadir a clasificación.
    c. Seleccione el proceso de clasificación y pulse Guardar.
    d. Opcionalmente, pulse Editar/Ver para modificar o ejecutar el proceso de clasificación.
    e. Si desea habilitar la auditoría de objetos de forma automática para todos los objetos encontrados por el proceso de clasificación, pulse **Editar/Ver** para abrir el proceso de clasificación; en la cinta Área de búsqueda, seleccione el recuadro de selección Habilitar la auditoría de objetos para bases de datos en la nube.
    f. Como alternativa, ejecute la clasificación: pulse Ejecutar ahora en la cinta Ejecutar descubrimiento en Descubrir > Escenarios integrales > Descubrir datos confidenciales.
2. Cree un nuevo proceso de clasificación y asígnele uno o más orígenes de datos.
    a. Seleccione uno o más orígenes de datos.
    b. Pulse Clasificación > Crear clasificación.
    c. Siga el procedimiento en Descubrir datos confidenciales.Habilitar la auditoría de objetos para bases de datos en la nube está seleccionado de forma predeterminada. Déjelo seleccionado.
    d. Ejecute la clasificación: Después de definir el Área de búsqueda, pulse Ejecutar ahora, o después de guardar el proceso, pulse Ejecutar ahora en la cinta Ejecutar descubrimiento.
3. Asigne uno o más orígenes de datos a un asesoramiento de vulnerabilidades existente.
    a. Seleccione uno o más orígenes de datos.
    b. Pulse Asesoramiento de vulnerabilidades > Añadir a asesoramiento de vulnerabilidades.
    c. Seleccione el proceso de asesoramiento de vulnerabilidades y pulse Guardar.
    d. Ejecute el proceso: Navegue a Reforzar > Asesoramiento de vulnerabilidades > Creador de asesoramientos, seleccione el proceso y pulse Ejecutar una vez ahora.
4. Cree un nuevo proceso de asesoramiento de vulnerabilidades y asígnele uno o más orígenes de datos.
    a. Seleccione uno o más orígenes de datos.
    b. Pulse Asesoramiento de vulnerabilidades > Crear asesoramiento de vulnerabilidades.
    c. Especifique una descripción del asesoramiento de vulnerabilidad; especifique una o varias direcciones de correo electrónico, separadas por comas, para recibir los resultados como parte de un proceso de auditoría que defina.
    d. Pulse Guardar.
    El proceso de VA se crea con todas las pruebas, los orígenes de datos seleccionados y los destinatarios que ha definido.
    e. Ejecute el proceso: Navegue a Reforzar > Asesoramiento de vulnerabilidades > Creador de asesoramientos, seleccione el proceso y pulse Ejecutar una vez ahora.

Tema principal: Protección del servicio de base de datos en la nube

Configurar la auditoría de bases de datos

Habilitar la auditoría en la base de datos para que los datos de auditoría de objetos los pueda extraer Guardium. Modificar el límite de objetos añadidos automáticamente a la clasificación y modificar el recopilador.

Acerca de esta tarea

La tabla de bases de datos presenta varios detalles de las bases de datos descubiertas. Puede utilizar los indicadores de color en la tabla para ver el estado de cualquier origen de datos de forma rápida. El color rojo indica que no hay ninguna configuración, por ejemplo, la base de datos no está catalogada o el origen de datos no se ha asignado a una clasificación o proceso de VA. Existen sugerencias de ayuda contextual en los indicadores de estado codificados por color para proporcionarle más información cuando el color es rojo o amarillo. Utilice la lista de filtros predefinidos para filtrar cualquiera de las columnas con indicadores de estado codificados por colores o el filtro de texto libre para otros valores.

Si hay un recopilador definido para el origen de datos, aparece en la columna Recopilador activo si usted es el propietario. De lo contrario, la columna aparecerá en blanco.

El propietario de auditoría de BD es el nombre de host del Gestor central en un entorno de Gestor central. En un sistema autónomo el valor es el nombre de host del recopilador.

La columna de Auditoría de base de datos tiene uno de los valores siguientes.

- Habilitado. Cuando viene seguido por un reinicio pendiente, indica que el estado será efectivo después del reinicio de la instancia.
- Inhabilitado. Cuando viene seguido por un reinicio pendiente, indica que el estado será efectivo después del reinicio de la instancia.
- La configuración no satisface el requisito. (El seguimiento de auditoría del parámetro AWS no está configurado de acuerdo al XML de requisito de Guardium, EXTENDED. Solicite su DBA que modifique este valor). Cuando viene seguido por un reinicio pendiente, indica que el estado será efectivo después del reinicio de la instancia.
- No soportado para este motor de base de datos. Actualmente Guardium no da soporte a la supervisión de actividad.

Si es el propietario de la instancia, se asigna un proceso de clasificación y se habilita la auditoría de la base de datos, debería ver los resultados en la columna de Objetos. El total es el número de objetos que los procesos de clasificación asignados a esta instancia han identificado; Auditado es el número de estos objetos que están habilitados para la Auditoría de objetos; Nuevo es el número de objetos encontrados por los procesos de clasificación pero que no se han habilitado de forma automática. Es preciso revisar estos objetos. Consulte Gestionar auditoría de objetos.

Debería ver los resultados en la columna `Objetos` si el origen de datos está asignado a un proceso de clasificación, si el proceso se ha ejecutado puesto que se habilitó la auditoría de bases de datos y si usted es el propietario. Si no ve los objetos, verifique el proceso de clasificación y vuelva a ejecutarlo.

Tema principal: Protección del servicio de base de datos en la nube

Modificar el límite de objetos añadidos automáticamente y el recopilador

Puede modificar el límite de objetos añadidos automáticamente y el recopilador en una o más bases de datos simultáneamente. Los campos que se dejan en blanco no se modifican.

Procedimiento

1. Seleccione una o más bases de datos.
2. Pulse Auditoría de base de datos > Configuración de auditoría de base de datos.
3. Modifique el número de Limitar objetos añadidos automáticamente. Este es el número máximo de objetos encontrados por clasificación que pueden habilitarse automáticamente para la auditoría de objetos, cuando la auditoría de base de datos está habilitada. Puede modificarlo, por base de datos, después de ser descubiertas. Los objetos que se habilitan automáticamente aparecen como Habilitado en la ventana de objetos gestionados. Si desea que Guardium añada objetos automáticamente, establezca un límite alto pero razonable de lo que espera que encuentre el proceso de clasificación. Para evitar un desbordamiento de objetos si hay un error en su clasificación, no establezca un valor demasiado alto. (Un desbordamiento podría afectar al rendimiento de la base de datos). Cero (0) significa que no se habilitarán objetos automáticamente para la auditoría de objetos. Si el número de objetos auditados más el número de objetos acabados de clasificar supera este límite, no se habilitan nuevos objetos para la auditoría de objetos. Por ejemplo, si lo establece en 15 y la clasificación identifica 5 objetos la primera vez que se ejecuta, se asignan 5 objetos al seguimiento de auditoría. Si se establece en 15 y hay 5 objetos ya habilitados para la auditoría de objetos y la próxima ejecución de clasificación identifica 16 objetos, no se habilita ningún objeto para la auditoría de objeto. Si se establece en 15 y hay 5 objetos ya habilitados para la auditoría de objetos y la próxima ejecución de clasificación identifica 5 objetos, los 5 nuevos objetos se habilitan para la auditoría de objetos.
4. El recopilador aparece en un entorno de Gestor central y es obligatorio. Seleccione un recopilador en la lista desplegable de todos los recopiladores en el entorno del Gestor central. Este es el recopilador que extrae los datos de auditoría (actividades) desde la base de datos.
5. Pulse Aplicar.

Habilitar la auditoría en una base de datos

Puede habilitar la auditoría de base de datos en una base de datos una a una.

Acerca de esta tarea

Puede configurar el parámetro Limitar objetos añadidos automáticamente o el recopilador con cualquier nivel de permisos. Otros cambios requieren permisos de base de datos. Es posible que sus claves de acceso no incluyan estos permisos. Las instrucciones siguientes cubren todos los niveles de permiso.

Cuando habilita una auditoría de base de datos, su sistema Guardium se vuelve el propietario exclusivo de la auditoría de base de datos en esta base de datos. Ningún otro sistema Guardium modifica la auditoría de base de datos o de objeto. Otro sistema puede tomar por la fuerza la propiedad pulsando Poseer auditoría de base de datos.

Ejecute la clasificación al menos una vez después de habilitar la auditoría de base de datos para ver y gestionar los objetos para la auditoría. Si no se encuentra ningún objeto, compruebe sus políticas.

PRECAUCIÓN:
Cuando empiece a gestionar la base de datos, se crea la etiqueta RDS de Amazon IBM Guardium IP con el valor de su nombre de host de Guardium. Esta etiqueta no se debe modificar o eliminar.

Procedimiento

1. Seleccione la fila de la base de datos.
2. Pulse Auditoría de base de datos > Configuración de auditoría de base de datos.

3. Opcionalmente, modifique el valor de los objetos añadidos automáticamente a la auditoría de objeto.
4. En un entorno del Gestor central (CM), si no hay ningún recopilador definido, seleccione uno de la lista desplegable y pulse en Aplicar. El diálogo se renueva y los botones se habilitan.
5. Si Habilitar auditoría de base de datos está habilitado, púlselo. El diálogo y la tabla se renovarán mostrando que usted es ahora el propietario de la auditoría de base de datos. El recuadro de diálogo se renueva. Pulse Reiniciar para reiniciar la base de datos ahora (aparece un mensaje de confirmación) o pulse Esperar el siguiente reinicio manual por ejemplo, para esperar una ventana de mantenimiento. Si elige Esperar al siguiente reinicio manual, debe acceder a la consola en la nube directamente más adelante. Si pulsa Reiniciar y no tiene suficientes derechos de acceso, aparece un error. Solicite a su administrador de base de datos configurar el **seguimiento de auditoría** como XML, EXTENDED y reinicie la instancia.
6. Si Habilitar auditoría de base de datos no está habilitado, pulse Poseer auditoría de base de datos. El recuadro de diálogo se renueva. Pulse Esperar el siguiente reinicio manual y solicite a su administrador de base de datos que configure el **seguimiento de auditoría** como XML, EXTENDED y reinicie la instancia.
7. Si ha realizado cambios en el estado de auditoría de la base de datos, pulse Recuperar estado y espere a que cambie el mensaje que indica el estado y, a continuación, pulse Renovar. La columna Propietario de auditoría de BD muestra el nombre de host del Gestor central (CM) o recopilador en un Guardium autónomo y el icono de auditoría de BD pasa a estar en verde.

Inhabilitar la auditoría en una base de datos

Puede inhabilitar la auditoría de base de datos en una base de datos una a una. Cuando inhabilita la auditoría de base de datos, también renuncia a la propiedad de la auditoría.

Acerca de esta tarea

Cuando deja de poseer o inhabilita la auditoría de base de datos, se inhabilita toda la auditoría de objetos y se suprime la lista de objetos que se pueden auditar (que procede de los resultados de clasificación).

Procedimiento

1. Seleccione la fila de la base de datos.
2. Pulse Auditoría de base de datos > Configuración de auditoría de base de datos.
3. Pulse Inhabilitar auditoría de base de datos, a continuación, pulse Esperar el siguiente reinicio manual, por ejemplo, para esperar una ventana de mantenimiento o pulse Reiniciar para reiniciar la base de datos ahora. Si elige Esperar al siguiente reinicio manual, debe acceder a la consola en la nube directamente más adelante. Si no tiene permiso para cambiar la configuración, pulse Dejar de poseer auditoría de base de datos y solicite a su administrador de base de datos que inhabilite la auditoría de base de datos en esta instancia.
4. Pulse Recuperar estado para renovar la pantalla con el último estado de la nube.

Resultados

Si hubo cambios, aparece un mensaje: `El estado de auditoría de base de datos ha cambiado para algunas bases de datos. Pulse Actualizar para actualizar la tabla.` Pulse Actualizar. El estado cambia a inhabilitado o inhabilitado pendiente de reinicio, el icono de la auditoría de base de datos se vuelve rojo y la columna Propietario de auditoría de BD aparecerá en blanco.

Poseer o dejar de poseer la auditoría de bases de datos

Acerca de esta tarea

Puede modificar el estado de la propiedad de una base de datos en un momento dado.

Ser el propietario de la auditoría de BD le proporciona derechos exclusivos para las definiciones de auditoría de BD y de objetos y acceso a los datos de auditoría de objeto. (Consulte Gestionar auditoría de objetos). Otros sistemas Guardium pueden acceder a la misma cuenta en la nube pero solo pueden ver los detalles de BD.

Con derechos de acceso completos, cuando habilita la auditoría de BD, también asume la propiedad de la BD. Si sus claves de acceso no proporcionan derechos de acceso completos, debe tomar la propiedad sin habilitar la auditoría de la BD. Cuando la auditoría de BD está habilitada (por el administrador de base de datos) debería tener acceso a los datos de auditoría. Por el contrario, cuando inhabilita la auditoría de BD, renuncia a la propiedad. Si su clave de acceso no proporciona derechos completos, debería dejar de poseer la auditoría y solicitar al administrador de base de datos que inhabilite la auditoría de BD.

Puede traspasar la propiedad de un sistema de Guardium a otro.

Si está transfiriendo la propiedad entre dos sistemas activos, primero detenga el propietario de la auditoría de la base de datos en el propietario actual, luego tome posesión de la propiedad en el segundo sistema Guardium. La auditoría se detiene cuando un sistema Guardium renuncia a su propiedad. Necesitará definir el proceso de auditoría en el nuevo sistema Guardium: asignar la base de datos a una clasificación, ejecutar el proceso y añadir objetos a la Auditoría de objetos.
PRECAUCIÓN:
Deje de poseer la auditoría de la base de datos en uno antes de iniciar su posesión en el segundo. Si no lo hace, los datos irán al recopilador anterior, así como al nuevo recopilador. Dos recopiladores con políticas distintas (diferentes CM) recibiendo las mismas actividades, producen resultados diferentes, o incompletos, en cada recopilador.

Si está transfiriendo la propiedad desde un sistema Guardium que se ha caído sin una expectativa de recuperación, puede iniciar la posesión de la auditoría de la base de datos desde otro sistema Guardium, manteniendo las definiciones de auditoría, sólo los cambios de propiedad. En este escenario, haga que el Guardium original deje de poseer la auditoría de la base de datos en la consola de base de datos.

Procedimiento

1. En la tabla de bases de datos, seleccione la fila de la base de datos.
2. Para dejar de poseer la auditoría de BD: Pulse Auditoría de base de datos > Configuración de auditoría de base de datos > Dejar de poseer auditoría de base de datos.
3. Para poseer la auditoría de BD: Pulse Auditoría de base de datos > Configuración de auditoría de base de datos > Poseer auditoría de base de datos.

Gestionar auditoría de objetos

Visualizar los objetos potencialmente confidenciales identificados por los procesos de clasificación en las bases de datos que gestiona y habilitar la auditoría de objetos en los objetos seleccionados para supervisar todas las actividades realizadas en esos objetos.

Acerca de esta tarea

Requisito previo: La auditoría de BD debe estar habilitada y, usted debe ser el propietario y la clasificación se debe ejecutar por lo menos una vez en este origen de datos.

Los nuevos objetos son aquellos que han encontrado los procesos de clasificación y que no se han habilitado para auditoría. Puede filtrar todos los objetos nuevos y, a continuación, habilitarlos para la auditoría de objetos o borrar el distintivo `Nuevo`. Cuando no hay Nuevos objetos, está al día con la evaluación de los objetos nuevos. Recuerde, Guardium puede recibir datos nuevos cada vez que se ejecuta el proceso de clasificación. Cuando se encuentran nuevos objetos que no se añadieron automáticamente a la auditoría de objetos, hay un aviso `Se han encontrado nuevos objetos`.

La columna `Se ha encontrado por clasificación` lista todos los procesos de clasificación que han identificado este objeto.

El estado Mixto en la columna Estado de auditoría de objetos significa que la auditoría de objetos está habilitada en algunos orígenes de datos e inhabilitada en otros.

Habilitar e inhabilitar la auditoría de objetos es un proceso intensivo y puede tardar unos minutos. Hay un icono de espera mientras la nube procesa los cambios de la auditoría.

Puede revisar objetos encontrados en uno o varios orígenes de datos seleccionando las filas de los orígenes de datos que desee revisar en la tabla de bases de datos. La ventana de auditoría de objetos muestra todos los objetos encontrados por todos los procesos de clasificación en la base o las bases de datos seleccionadas.

- Gestión de auditoría de objetos en una base de datos
- Gestión de auditoría de objetos en varias bases de datos

Tema principal: Protección del servicio de base de datos en la nube

Gestión de auditoría de objetos en una base de datos

Acerca de esta tarea

La ventana Objetos en origen de datos <nombre> lista todos los objetos encontrados por la ejecución de los procesos de clasificación en este origen de datos. Los objetos pueden ser encontrados por más de un proceso de clasificación.

Cuando el proceso de clasificación ha identificado objetos pero no los habilita automáticamente para la auditoría de objetos, aparece `Se han encontrado nuevos objetos` sobre la tabla de objetos. Pulse Sólo nuevo para filtrar los objetos encontrados nuevos que requieren gestión. Se podrían encontrar objetos nuevos cada vez que se ejecuta la clasificación. Cuando no hay Nuevos objetos, está al día con la evaluación de los objetos nuevos.

Revise periódicamente los orígenes, buscando objetos nuevos y, opcionalmente, añadiendo o eliminando objetos de la auditoría de objetos. Por ejemplo, puede eliminar objetos si los objetos añadidos automáticamente incluyen objetos que ha decidido que no necesitan de auditoría o si una base de datos está teniendo problemas de rendimiento. O puede identificar un objeto sospechoso que no se ha auditado y añadirlo a la auditoría de objetos.

Utilice el filtro de clasificación para los objetos que sabe que se deben auditar. Seleccione todos los objetos en la vista filtrada y habilite la auditoría de objetos.

Procedimiento

1. Si ha asignado el proceso de clasificación **antes** de habilitar la auditoría de bases de datos, ejecute la clasificación una vez ahora y espere unos minutos (o espere la siguiente ejecución planificada) para que Guardium identifique los objetos.
2. Seleccione un origen de datos. Considere utilizar el filtro Se han encontrado nuevos objetos para identificar orígenes de datos con nuevos objetos.
3. Seleccione Auditoría de base de datos > Gestionar auditoría de objetos. Se abre la ventana Gestionar auditoría de objetos que lista todos los objetos encontrados por los procesos de clasificación a los que está asignado el origen de datos.
4. Considere utilizar el filtro Sólo nuevo para identificar todos los objetos clasificados como Nuevo.
5. Seleccione uno o más objetos (filas) en la tabla.
6. Para habilitar el seguimiento de auditoría, seleccione Acciones > Habilitar auditoría. El sistema responde con el éxito o el fracaso de la operación.
7. Para borrar el distintivo nuevo, pulse Acciones > Borrar nuevo distintivo.
8. Para inhabilitar el seguimiento de auditoría, seleccione Acciones > Inhabilitar auditoría . El sistema responde con el éxito o el fracaso de la operación.

Tema principal: Gestionar auditoría de objetos

Gestión de auditoría de objetos en varias bases de datos

Acerca de esta tarea

Esta vista lista todos los objetos encontrados por los procesos de clasificación ejecutados en los orígenes de datos seleccionados. Los objetos pueden ser encontrados por más de un proceso de clasificación. Visualice los objetos agrupados por objeto (predeterminado) o clasificación. La columna Se ha encontrado por clasificación lista todos los procesos de clasificación que han identificado el objeto.

Cuando el proceso de clasificación identifica objetos pero no los habilita automáticamente para la auditoría de objetos, aparece Se han encontrado nuevos objetos sobre la tabla de objetos. Pulse Sólo nuevo para filtrar los objetos encontrados nuevos que requieren gestión. Revise los Objetos nuevos y habilite la auditoría de objetos o borre el distintivo Nuevo.

Se podrían encontrar objetos nuevos cada vez que se ejecuta la clasificación. Cuando no hay Nuevos objetos, está al día con la evaluación de los objetos nuevos.

Revise periódicamente los orígenes, buscando objetos nuevos y, opcionalmente, añadiendo o eliminando objetos de la auditoría de objetos. Por ejemplo, puede eliminar objetos si los objetos añadidos automáticamente incluyen objetos que ha decidido que no necesitan de auditoría o si una base de datos está teniendo problemas de rendimiento. O puede identificar un objeto sospechoso que no se ha auditado y añadirlo a la auditoría de objetos.

Agrupar por objeto: Para ver todos los nuevos objetos encontrados, escriba Nuevo en el filtro de texto.

Para habilitar o inhabilitar la auditoría de objetos en un objeto en todos los orígenes de datos seleccionados, seleccione las filas y pulse Acción y Habilitar o Inhabilitar.

Para llevar a cabo una acción por origen de datos, pulse Presente en orígenes de datos para ver todos los orígenes de datos cuyos procesos de clasificación hayan identificado el objeto seleccionado.

Agrupar por clasificación es especialmente útil cuando tiene orígenes de datos casi idénticos, o políticas de clasificación, cuyos objetos necesitan auditoría sin ninguna otra evaluación, por ejemplo, GDPR.

Procedimiento

1. Si ha asignado el proceso de clasificación **antes** de habilitar la auditoría de bases de datos, ejecute la clasificación una vez ahora (o espere a la siguiente ejecución planificada) y espere unos minutos para que Guardium identifique los objetos.
2. Cuando se agrupa por objeto:
    a. Seleccione varios orígenes de datos con Nuevos objetos en la columna de Objetos de la Tabla de bases de datos. Utilice el filtro Se han encontrado nuevos objetos para identificar estos orígenes de datos.
    b. Pulse Auditoría de base de datos > Gestionar auditoría de objetos. Se abre la ventana Gestionar auditoría de objetos.
    c. Si se debe auditar siempre el objeto en todos los orígenes de datos, seleccione las filas y pulse Acciones > Habilitar auditoría. El sistema responde con el éxito o el fracaso de la operación.
    d. Si desea habilitar la auditoría de objetos en bases de datos individuales, pulse el número en la columna Presente en orígenes de datos en la fila del objeto para abrir la ventana Orígenes de datos que contienen <objeto>. Esta ventana muestra todos los orígenes de datos cuyos procesos de clasificación han identificado el objeto seleccionado. Seleccione una o más columnas de orígenes de datos y pulse Acciones > Habilitar auditoría.
3. Para un proceso de clasificación cuyos objetos identificados siempre necesitan auditoría sin posterior evaluación: Pulse el botón de selección Clasificación (encima de la tabla); seleccione una o varias filas de procesos de clasificación y pulse Acciones > Habilitar auditoría.

Tema principal: Gestionar auditoría de objetos

Descubrimiento automático de base de datos

La aplicación de descubrimiento automático escanea y sondea sus servidores en busca de puertos abiertos para impedir las conexiones no deseadas o desconocidas a su red. Puede ejecutar procesos de descubrimiento automático a petición o planificar el proceso de forma periódica.

Visión general del descubrimiento automático de base de datos

Hay muchos escenarios en los que pueden existir bases de datos sin ser detectadas en su red y exponer su red a riesgos potenciales. Es posible que las bases de datos antiguas se olviden y no se supervisen o es posible que se añada una nueva base de datos como parte de un paquete de aplicaciones. Es posible que un administrador de base de datos esporádico cree también una nueva instancia de una base de datos para realizar actividades maliciosas fuera de las bases de datos supervisadas.

El descubrimiento automático utiliza trabajos de escaneo y sondeo para asegurarse de que no hay ninguna base de datos no detectada en su entorno.

- Un trabajo de *escaneo*, escanea cada host especificado (o hosts en una subred especificada) y recopila una lista de puertos abiertos especificados para ese host.
- Un trabajo de *sondeo* utiliza los resultados del escaneo para determinar si hay servicios de base de datos ejecutándose en los puertos abiertos. Un trabajo de sondeo no se puede completar sin ejecutar primero un escaneo. Visualice los resultados de este trabajo en el informe predefinido de Bases de datos descubiertas.

Antes de empezar, debe bajar e instalar el parche para la aplicación de descubrimiento automático. El parche está disponible en IBM Fix Central.

Siga estos pasos para utilizar la aplicación descubrimiento automático:

1. Cree un proceso de descubrimiento automático para buscar puertos abiertos en direcciones IP específicas o subredes.
2. Ejecute el proceso de descubrimiento automático a petición o de una forma planificada.
3. Visualice los resultados del proceso con los informes de descubrimiento automático o cree informes personalizados.

El descubrimiento automático tiene sus propios procesos que son independientes de los procesos de auditoría, pero funcionan exactamente de la misma manera que los procesos de auditoría.

Solo puede especificar direcciones IP al realizar un escaneo y no nombres de host, sin embargo Guardium detecta nombres de host como parte del informe. Guardium no trunca los nombres de host en el producto Guardium. Es posible que tenga que configurar el informe para que tenga columnas más anchas.

El descubrimiento automático de Guardium no adivina en qué base de datos aparece durante un sondeo. Si el descubrimiento automático de Guardium dice que ha encontrado una base de datos, es seguro al 100% de que es la base de datos.

Nota: El descubrimiento solo encuentra bases de datos en ejecución. Será necesario iniciar las bases de datos si se va a utilizar el descubrimiento durante la instalación. Debido al funcionamiento de la interceptación AIX KTAP, las bases de datos deben reiniciarse después de la primera vez que se ejecuta S-TAP. Si no se reinician las bases de datos, algunas interceptaciones no funcionarán.

Crear un proceso de descubrimiento automático

Especifique qué host y puertos escanea el proceso de descubrimiento automático.

1. Configure el descubrimiento automático pulsando Descubrir > Descubrimiento de base de datos > Configuración de descubrimiento automático.
2. Pulse Nuevo para crear un nuevo proceso y abra el Creador de proceso de descubrimiento automático.
3. Especifique un Nombre de proceso que sea exclusivo en su sistema Guardium.
4. Para ejecutar un trabajo de sondeo inmediatamente después de completar el trabajo de escaneo, marque el recuadro de selección Ejecutar sondeo después de escaneo.
5. Para cada host o subred que se vaya a escanear, especifique el host y puerto y pulse Añadir escaneo. Cada vez que añade un escaneo se añade a la lista de tareas. Nota:
    - Los caracteres comodín están habilitados. Por ejemplo: Para seleccionar todas las direcciones que empiezan por 192.168.2, utilice 192.168.2.*.
    - Especifique un rango de puertos colocando un guion entre el primer y el último número de puerto en el rango. Por ejemplo: 4100-4102.
    - Después de añadir un escaneo, modifique el host o puerto escribiendo sobre el mismo. Pulse Aplicar para guardar las modificaciones.
    - Si tiene una configuración de pila dual, deberá configurar un escaneo para las direcciones IPV4 e IPV6.
    - Para eliminar un escaneo, pulse el icono Suprimir esta tarea para el escaneo. Si una tarea tiene resultados de escaneo que dependen de ella, el escaneo no se puede suprimir.
6. Cuando haya terminado de añadir escaneos, pulse Aplicar y ejecute el trabajo o planifique el trabajo en el futuro.

Consulte Planificación si necesita definir una planificación.

Ejecute un proceso de descubrimiento automático

Ejecute o planifique trabajos de escaneo y sondeo como parte del proceso de descubrimiento automático.

1. Pulse Descubrir > Descubrimiento de base de datos > Configuración de descubrimiento automático.
2. Seleccione el proceso a ejecutar desde la lista Selector de proceso de descubrimiento automático y realice una de las acciones siguientes:
3.
    - Para ejecutar un trabajo inmediatamente, pulse Ejecutar una vez ahora.
    - Para planificar un trabajo en el futuro, pulse Modificar planificación (consulte Planificación si necesita ayuda para definir una planificación).
      Nota: No se puede ejecutar un trabajo de sondeo sin los resultados del trabajo de escaneo. Puede planificar los dos trabajos para que se ejecuten individualmente o configurar el trabajo de sondeo para que se ejecute después del trabajo de escaneo modificando un proceso y marcando el recuadro de selección Ejecutar sondeo después de escaneo.
4. Después de iniciar o planificar un trabajo, puede pulsar Resumen de progreso para visualizar el estado de este proceso.

Informes de descubrimiento automático

Abra el informe del descubrimiento automático pulsando Descubrir > Informes y selecciónelo en la lista de informes disponibles.

Puede crear informes personalizados con el Creador de consultas de descubrimiento automático. Abra el Creador de consultas de descubrimiento automático pulsando Descubrir > Descubrimiento de base de datos > Creador de consultas de descubrimiento automático.

Informe de bases de datos descubiertas

Abra el informe de Bases de datos descubiertas pulsando Descubrir > Informes > Bases de datos descubiertas.

La entidad principal para este informe es el puerto descubierto. Cada puerto individual descubierto tiene su propia fila en el informe. Las columnas listadas son: Hora del análisis, Dirección IP del servidor, Nombre de host de servidor, Tipo de BD, Puerto, Tipo de puerto (normalmente TCP) y un recuento de las apariciones.

No hay parámetros de tiempo de ejecución especiales para este informe, pero excluye cualquier puerto descubierto con tipo de base de datos Desconocido.

Cuando cambia una definición de proceso de descubrimiento automático, las estadísticas de ese proceso se restablecen.

Dominio de seguimiento del descubrimiento automático

El dominio de seguimiento del descubrimiento automático contiene todos los datos informados por los procesos de descubrimiento automático. Pulse cualquier nombre de entidad para visualizar sus atributos.

Entidades del dominio de seguimiento del descubrimiento automático

- El escaneo de descubrimiento automático proporciona una indicación de fecha y hora para cada operación de escaneo.
- Los hosts descubiertos proporcionan la dirección IP y el nombre de host de cada host descubierto.
- Los puertos descubiertos proporcionan una indicación de fecha y hora, identifica el puerto y proporciona el tipo de base de datos para cada puerto descubierto abierto.

Tema principal: Descubrir

Clasificación

Los procesos y políticas de clasificación definen cómo Guardium descubre y trata los datos confidenciales como, por ejemplo, los números de tarjetas de crédito, números de la seguridad social y datos financieros personales.

Los procesos de descubrimiento y clasificación se vuelven importantes a medida que crece una organización y la información confidencial como, por ejemplo, los números de tarjeta de crédito y datos financieros personales pasan a estar presentes en varias ubicaciones, a menudo sin el conocimiento de los administradores actuales responsables de esos datos. Esto sucede con frecuencia en el contexto de las fusiones y las adquisiciones o cuando los sistemas existentes han durado más que los propietarios originales. Crear flujos de trabajo para descubrir datos confidenciales le permite identificar datos confidenciales en su entorno y tomar las medidas adecuadas, como, por ejemplo, aplicar políticas de acceso.

El *Proceso de clasificación* consiste en políticas de clasificación que se asocian con uno o más orígenes de datos. Los procesos de clasificación pueden someterse para ejecutarse una vez o, si se han almacenado credenciales de inicio de sesión para todas las bases de datos utilizadas en el proceso, planificar para ejecutarse de forma periódica en un proceso de automatización de flujo de trabajo de cumplimiento.

Las *políticas de clasificación* constan de reglas de clasificación y acciones de reglas de clasificación diseñadas para buscar y etiquetar datos confidenciales en orígenes de datos especificados.

Las *reglas de clasificación* utilizan expresiones regulares, algoritmos Luhn y otros criterios para definir reglas para el contenido coincidente al aplicar una política de clasificación.

Las *acciones de regla de clasificación* especifican un conjunto de acciones que se deben llevar a cabo para cada regla en una política de clasificación. Por ejemplo, una acción puede generar una alerta de correo electrónico o añadir un objeto a un grupo de Guardium. Cada vez que se cumple una regla, ese suceso se registra y, por lo tanto, se puede informar sobre él (a menos que se especifique ignorar como la acción a llevar a cabo, en cuyo caso no hay ningún registro para esa regla).

- Rendimiento del proceso de clasificación
  Los procesos de clasificación se gestionan con rutinas de ejemplo y parámetros de tiempo de espera que garantizan un impacto mínimo en el rendimiento en los servidores de bases de datos.
- Gestión de reglas de clasificación
  Las reglas de clasificación se gestionan de acuerdo con criterios flexibles de coincidencia y agrupación.
- Cómo trabajar con procesos de clasificación
  Crear, ejecutar y ver procesos de clasificación utilizando el Creador de procesos de clasificación.
- Cómo trabajar con políticas de clasificación
- Cómo trabajar con reglas de clasificación
- Cómo trabajar con acciones de regla de clasificación

Tema principal: Descubrir

Rendimiento del proceso de clasificación

Los procesos de clasificación se gestionan con rutinas de ejemplo y parámetros de tiempo de espera que garantizan un impacto mínimo en el rendimiento en los servidores de bases de datos.

Cuando se ejecuta el clasificador, tiene la opción de especificar como muestra los registros. El comportamiento predeterminado toma una muestra aleatoria de las filas utilizando una sentencia adecuada para la plataforma de base de datos en cuestión. Por ejemplo, el clasificador toma muestras utilizando una sentencia rand() para bases de datos SQL. El comportamiento alternativo es el muestreo secuencial, que lee filas, en orden, hasta el tamaño de muestra especificado. El muestreo aleatorio es el comportamiento predeterminado y, por lo general, se suele recomendar porque proporciona resultados más representativos. Sin embargo, es posible que el muestreo aleatorio origine un ligero descenso en el rendimiento si se compara con el muestreo secuencial. Tanto para el muestreo aleatorio como para el secuencial, el tamaño de la muestra es de 2000 filas o el número total de filas disponibles, lo que sea menor. Se pueden especificar tamaños de muestra más grandes o pequeños.

Para minimizar aún más el impacto del proceso de clasificación en el servidor de bases de datos, las consultas de larga ejecución se cancelarán, registrarán y se omitirá el resto de la tabla. Cualquier fila adquirida a partir de este punto, se utilizará mientras se evalúan reglas para la tabla. De forma similar, si un proceso de clasificación se ejecuta durante un amplio periodo de tiempo sin completarse, se detendrá todo el proceso, se registrará con las estadísticas de proceso y se iniciará el siguiente proceso de clasificación. Esto es poco habitual y normalmente solo ocurre en servidores que ya están experimentando problemas de rendimiento.

El clasificador se regula periódicamente para estar en reposo para que el servidor de bases de datos no colapse con solicitudes. Si hay muchas reglas de clasificación tomando muestras de datos, la carga en el servidor de bases de datos debería permanecer constante pero es posible que el proceso tarde más tiempo en ejecutarse.

El clasificador gestiona los falsos positivos mediante grupos excluidos para esquemas, tablas y columnas de tabla. Anteriormente, configurar Guardium para ignorar los resultados de falsos positivos en futuros escaneos de clasificación, podía ser un proceso complejo. Ahora, cuando revise los resultados del clasificador, puede añadir fácilmente resultados de falsos positivos a un grupo de exclusión y añadir ese grupo a la política de clasificación para asegurarse de que dichos resultados se ignoran en futuros escaneos.

Tema principal: Clasificación

Gestión de reglas de clasificación

Las reglas de clasificación se gestionan de acuerdo con criterios flexibles de coincidencia y agrupación.

Marcador Activar solo con

El marcador Activar solo con permite la agrupación de tipos reglas de clasificación por el mismo nombre. Además, todas las reglas devueltas que utilizan un marcador deben devolver datos basados en el mismo nombre de tabla. Si se definen dos o más reglas con el mismo marcador, estas reglas se activarán conjuntamente de modo que si se activan en la misma tabla, ambas se registrarán y se invocarán sus acciones. Si por el contrario, solo una de ellas se activa en una tabla, ninguna de las reglas se registrará o se invocarás sus acciones. Ser capaz de poder activar varias reglas conjuntamente se vuelve importante cuando se ocupa de datos confidenciales que aparecen juntos en la misma tabla. Por ejemplo, es posible que desee saber cuándo una tabla tiene un número de seguridad social y un carnet de conducir de Massachusetts.

El marcador Activar solo con es un valor constante, se puede elegir cualquier valor y debe tener exactamente el mismo valor en todas las reglas que desea agrupar. Esto significa que si una regla tiene un marcador ABC, la otra regla con la que desea agruparla debe tener también un marcador denominado ABC. Cualquier otro valor de marcador y las reglas no se agrupan.

Debe utilizar, por lo menos, dos reglas de cualquier valor basadas en la búsqueda de datos en el mismo nombre de tabla.

Continuar en coincidencia

El marcador Activar solo con también está basado en el Continuar en coincidencia. Como ejemplo, si se han definido las reglas de forma que la Regla 3 no coincida con el Continuar en coincidencia no se devolverán resultados a pesar de que las tres reglas de marcador fueran positivas. Esto se debe a que no se ha podido ejecutar la Regla 4 y no se activará la agrupación porque todos los marcadores Activar solo con deben ejecutarse y con resultados positivos.

Regla 1. Regla de marcador de activación ABC (Continuar en coincidencia)

Regla 2. Regla de marcador de activación ABC (Continuar en coincidencia)

Regla 3. Tipo de regla de no marcador de activación (Continuar en coincidencia)

Regla 4. Regla de marcador de activación ABC (Continuar en coincidencia)

Solo columnas no coincidentes

Utilice esta opción para reducir la granularidad de los resultados de datos. Es posible que algunas organizaciones deseen realizar una encuesta de sus datos para descubrir qué tablas y columnas tienen datos confidenciales sin necesidad de encontrar cada tipo de datos confidenciales en dicha columna. Una nueva opción para Continuar en coincidencia, Solo con columnas no coincidentes, significa que tan pronto como el clasificador encuentre una coincidencia en dicha columna la ignorará a medida que continúa su proceso.

Tabla 1. Resumen de opciones de proceso de clasificador disponibles

Continuar en coincidencia	Solo con columnas no coincidentes	Granularidad del resultado
No	N/D	Tabla. El clasificador detendrá las reglas de proceso después de la primera coincidencia en la tabla.
Sí	Sí	Tabla y columna. El clasificador registrará la primera coincidencia para cualquier columna y la ignorará en adelante para las reglas subsiguientes.
Sí	No	Detallado. El clasificador registrará las coincidencias de todas las columnas para todas las reglas.

Clasificación con el algoritmo de Luhn

Cuando un nombre de regla empieza con guardium://CREDIT_CARD y hay un patrón de número de tarjeta de crédito válido en el recuadro Expresión de búsqueda, la política de clasificación utilizará el algoritmo de Luhn (un algoritmo ampliamente utilizado para validar números de identificación como, por ejemplo, los números de tarjeta de crédito), además de la coincidencia de patrón estándar. El algoritmo de Luhn es una comprobación adicional y no reemplaza la comprobación de patrón. Un número de tarjeta de crédito válido es una serie de 16 dígitos o cuatro conjuntos de cuatro dígitos, separados por un espacio en blanco. Existe un requisito para tener el nombre de regla guardium://CREDIT_CARD y un número [0-9]{16} válido en el recuadro Expresión de búsqueda para implicar el algoritmo de Luhn en esta coincidencia de patrón.

Tema principal: Clasificación

Cómo trabajar con procesos de clasificación

Crear, ejecutar y ver procesos de clasificación utilizando el Creador de procesos de clasificación.

Procedimiento

Abra el Creador de procesos de clasificación navegando a Descubrir > Clasificaciones > Creador de procesos de clasificación.
Tema principal: Clasificación

Crear un proceso de clasificación

Procedimiento

1. Desde el Creador de procesos de clasificación, pulse el icono para abrir el panel Definir proceso de clasificación.
2. Especifique un nombre para el proceso en el campo Descripción de proceso.
3. Seleccione la política de clasificación de la lista. Puede pulsar Modificar para ver y editar la política si es necesario.
4. Opcionalmente, desmarque el recuadro de selección Muestreo aleatorio. Esta característica solo se aplica cuando el número de registros de una tabla sobrepasa el tamaño de la muestra. El muestreo aleatorio buscará aleatoriamente un número de registros en la tabla hasta el tamaño de muestra definido. Se trata de una búsqueda de alta calidad porque los resultados son más representativos. Al desmarcar el recuadro de selección Muestreo aleatorio cambia el comportamiento para buscar secuencialmente registros en la tabla hasta el tamaño de muestra definido. Es posible que una búsqueda secuencial sea más rápida que un muestreo aleatorio, pero los resultados pueden no ser tan representativos.
5. Especifique un Tamaño de la muestra al buscar datos (consulte Definir reglas de política de clasificación/Definir una regla Buscar datos), si el número de registros de una tabla es < = al "Tamaño de la muestra", se busca una coincidencia en todos esos registros. Cuando el número de registros en una tabla supera el "Tamaño de la muestra" se utiliza el muestreo aleatorio.
6. Pulse el botón Añadir origen de datos para añadir uno o más orígenes de datos.
7. Pulse Guardar. Esto completa la definición del proceso de clasificación.
8. Opcionalmente, añada comentarios a la definición. Consulte Comentarios en el manual de ayuda Herramientas comunes.
9. Opcionalmente, añada roles de seguridad. Consulte Roles en el manual de ayuda Gestión de acceso.
10. Opcionalmente, envíe el proceso de clasificación para su ejecución. Consulte Ejecutar un proceso de clasificación.
11. Pulse Hecho cuando haya terminado.

Ejecutar un proceso de clasificación

Acerca de esta tarea

Hay tres formas de ejecutar un proceso de clasificación:

- A petición, desde el Creador de procesos de clasificación, que se describe en esta tarea.
- Como tarea dentro del *Proceso de Automatización de flujo de trabajo de cumplimiento*, descrito en otro lugar.
- Como parte de un *Flujo de trabajo de Descubrir datos confidenciales*, descrito en otro lugar.

Procedimiento

1. Desde el Creador de procesos de clasificación, seleccione el proceso a ejecutar y pulse Modificar para abrir el Creador de procesos de clasificación.
2. Pulse el botón Ejecutar una vez ahora para enviar el trabajo. Esto coloca el proceso en la cola de trabajos de Guardium, desde la que el sistema Guardium ejecuta los trabajos uno a uno. Puede ver el estado del trabajo utilizando la Cola de trabajos de Guardium.
3. Pulse el botón Listo cuando haya terminado.

Ver los resultados de clasificación

Procedimiento

1. Desde el Creador de procesos de clasificación, pulse el botón Ver resultados. Los resultados se abrirán en una ventana aparte.
2. En cualquier fila del Registro de ejecución de procesos, pulse (detalles) para visualizar más información.
3. Opcionalmente, si la Seguridad de usuario de datos está habilitada, a través del Perfil global, se visualizarán los recuadros de selección que permiten a los usuarios controlar/conmutar filas en el conjunto de resultados de acuerdo con el Filtro definido.
4. Pulse Cerrar esta ventana cuando haya terminado de ver los resultados. Además, hay un informe de Registro de procesos de clasificador para visualizar el estado del proceso de clasificación.

Ver la cola de trabajos

Antes de empezar

La cola de trabajos de Guardium está disponible solo para el portal de administrador.

Procedimiento

Para ver el informe, abra la Cola de trabajos de Guardium navegando a Descubrir > Clasificaciones > Cola de trabajos de Guardium.

Cómo trabajar con políticas de clasificación

Procedimiento

Abra el Creador de políticas de clasificación navegando a Descubrir > Clasificaciones > Creador de procesos de clasificación.
Tema principal: Clasificación

Crear una política de clasificación

Procedimiento

1. Pulse Nueva para abrir el panel Definición de política de clasificación.
2. Especifique un nombre exclusivo en el campo Nombre.
3. Especifique una categoría en el campo Categoría y una clasificación en el campo Clasificación. Ambos son necesarios. Ambos se utilizan para agrupar y organizar datos en los informes.
4. Opcionalmente, especifique una descripción.
5. Opcionalmente, especifique comentarios. Se pueden especificar en cualquier momento después de guardar la política. Consulte Comentarios.
6. Pulse Editar reglas para definir reglas y sus acciones asociadas. Consulte Definir reglas de política de clasificación para obtener instrucciones detalladas. Se recomienda utilizar el escenario Descubrir datos confidenciales (Descubrir > Escenarios integrales > Descubrir datos confidenciales) para modificar políticas de clasificación existentes. Utilice el mismo escenario Descubrir datos confidenciales para crear grupos de políticas de clasificación. Además, si se han creado grupos, deben seleccionarse explícitamente.

Modificar una política de clasificación

Procedimiento

1. Seleccione la política de clasificación a modificar y realice una de las siguientes acciones:
   - Para modificar reglas de política, pulse Editar reglas y consulte Definir reglas de política de clasificación.
   - Para modificar cualquier otro elemento de la definición, pulse el botón Modificar.
2. Escriba encima de cualquiera de estos elementos según sea necesario.
3. Pulse Guardar para guardar los cambios y pulse Listo cuando haya terminado.

Clonar una política de clasificación

Procedimiento

1. Seleccione la política de clasificación a clonar y pulse en el botón Clonar:
2. Escriba encima de cualquiera de estos elementos según sea necesario para la política clonada. Recomendamos que reemplace el nombre predeterminado de la política clonada, que es el nombre de la política seleccionada con el prefijo Copia de.
3. Pulse el botón Guardar clon para guardar la nueva política de clasificación. La política se volverá a visualizar en el panel Definición de política de clasificación.
4. Consulte Modificar una política de clasificación para obtener instrucciones sobre cómo cambiar componentes de la nueva definición de política de clasificación.

Cómo trabajar con reglas de clasificación

Procedimiento

1. Abra el panel Reglas de política de clasificación desde el Buscador de políticas de clasificación navegando a Descubrir > Clasificaciones > Creador de políticas de clasificación.
2. Se recomienda utilizar el escenario Descubrir datos confidenciales (Descubrir > Escenarios integrales > Descubrir datos confidenciales) para modificar políticas de clasificación existentes. Utilice el mismo escenario Descubrir datos confidenciales para crear grupos de políticas de clasificación. Además, si se han creado grupos, deben seleccionarse explícitamente.

Tema principal: Clasificación

Añadir una nueva regla de política de clasificación

Procedimiento

1. Pulse el botón Añadir regla para abrir el panel Definición de regla de clasificación.
2. Especifique un nombre de regla.
3. Opcionalmente, especifique una nueva categoría y/o clasificación para la regla. Los valores predeterminados se toman de la Definición de regla de clasificación de la política.
4. Si la siguiente regla en la política de clasificación debe evaluarse después de que coincida, marque el recuadro de selección Continuar en coincidencia. De forma predeterminada, se dejan de evaluar las reglas cuando la regla coincide.
5. Seleccione un tipo de regla. Para una regla nueva, no hay un tipo de regla seleccionado. Una vez se ha seleccionado el tipo de regla, el panel se amplía para incluir los campos necesarios para definir ese tipo de regla. Para conocer las especificaciones de cómo definir cada tipo de regla, consulte una de las siguientes secciones:
   - Definir una regla Búsqueda de catálogo: Busca el nombre de columna o tabla en el catálogo de bases de datos.
   - Definir una regla Buscar datos: Compara valores específicos o patrones en los datos.
     Nota: La autenticación de base de datos (usuario/contraseña) definida en la definición del origen de datos utilizada debe tener los niveles de permisos adecuados para la regla/búsqueda que se está definiendo. Por ejemplo, en Oracle, un usuario con un rol adecuado (como SYSTEM o DBA) puede buscar correctamente un derecho de acceso dentro del catálogo de bases de datos. Esta nota se aplica a la elección Tabla del sistema al utilizar el tipo de regla Buscar datos. No comprueba la Tabla del sistema si el usuario no tiene el rol SYSTEM.
   - Definir una regla Buscar datos no estructurados: Compara valores específicos o patrones en un archivo de datos no estructurados (CSV, Texto, HTTP, HTTPS, Samba)
6. Pulse el botón Nueva acción para añadir una acción a realizar cuando esta regla coincida. Consulte Añadir una acción de regla de clasificación.
7. Pulse Aceptar para añadir la regla a la política.

Definir una regla de búsqueda de catálogo

Acerca de esta tarea

Una regla de búsqueda de catálogo busca en el catálogo de bases de datos los nombres de tabla o de columna que coincidan con los patrones especificados. Se permiten los comodines: % para cualquier número de caracteres o _ (guion bajo) para un único carácter.

Procedimiento

1. En la fila Tipo de tabla, marque por lo menos un tipo de tabla a buscar: Sinónimo, Tabla o Vista. (Tabla está seleccionado de forma predeterminada).
2. Opcionalmente, especifique un nombre específico o un patrón basado en comodines en el recuadro Nombre de tabla como. Si se omite, se seleccionarán todos los nombres de tabla.
3. Opcionalmente, especifique un nombre específico o un patrón basado en comodines en el recuadro Nombre de columna como. Si se omite, se seleccionarán todos los nombres de columna.
4. Pulse el botón Aceptar cuando haya terminado.

Definir una regla Buscar datos

Acerca de esta tarea

Una regla Buscar datos busca en una o más columnas los valores de datos específicos. Se permiten los comodines: % para cualquier número de caracteres o _ (guion bajo) para un único carácter. Por ejemplo, el tipo de regla es Buscar datos, el tipo de tabla es Tabla y el Nombre de tabla como es CREDIT%.

Procedimiento

1. En la fila Tipo de tabla, marque por lo menos un tipo de tabla a buscar: Sinónimo, Tabla o Vista. (Tabla está seleccionado de forma predeterminada).
2. En la fila Nombre de tabla como, opcionalmente, especifique un nombre específico o un patrón basado en comodines. Si se omite, se seleccionarán todos los nombres de tabla.
3. En la fila Tipo de datos, seleccione uno o más tipos de datos en los que buscar.
4. En la fila Nombre de columna como, opcionalmente, especifique un nombre específico o patrón de comodines. Si se omite, se seleccionarán todos los nombres de columna.
5. Opcionalmente, especifique la longitud mínima. Si se omite, no hay límite.
6. Opcionalmente, especifique la longitud máxima. Si se omite, no hay límite.
7. En el campo Búsqueda con like, opcionalmente, especifique un valor específico o un patrón basado en comodines. Si se omite, se seleccionarán todos los valores.
8. En el campo Expresión de búsqueda, opcionalmente, especifique una expresión regular para definir un patrón para que coincida. Para probar una expresión regular, pulse el botón (expresión regular) para abrir el panel Crear expresión regular en una ventana separada. Para obtener información detallada sobre cómo utilizar expresiones regulares, consulte Expresiones regulares.
9. En el Nombre de evaluación, opcionalmente, especifique un nombre de clase Java™ completo que se haya creado y subido. A continuación, se utilizará la clase Java para activar y evaluar la serie. No hay ninguna validación de que el nombre de clase especificado se haya cargado y se ajuste a la interfaz. Consulte Evaluación personalizada y Gestionar clases personalizadas para obtener más información sobre la creación y la subida de archivos de clase Java.
10. Opcionalmente, especifique un nombre de marcador Activar solo con. Consulte, Marcador Activar solo con.
11. En el campo Porcentaje de aciertos, opcionalmente especifique un porcentaje de datos coincidentes que se deba conseguir para que se active esta regla. Se devuelven los datos si el porcentaje de datos coincidentes examinado es mayor o igual (>=) que el valor de porcentaje especificado, tenga en cuenta que una entrada vacía significa que no hay una condición y no afectará si la regla se activa o no y devuelve datos a la pantalla de la vista. Un porcentaje de 0 hará que la regla se active para esta condición y devuelva datos a la pantalla de la vista y un porcentaje de 100 requiere que todo coincida.
12. En el campo Comparar con valores en SQL, opcionalmente, especifique una sentencia SQL. El SQL especificado, que debe estar basado en la información de retorno de una sola columna, se utilizará como grupo de valores para buscar en las tablas y/o columnas seleccionadas. Si se utiliza, Comparar con valores en SQL, debería seguir las siguientes reglas:
    - La sentencia SQL DEBE empezar con SELECT.
    - La sentencia SQL NO DEBE utilizar ';' punto y coma.
    - El SQL especificado DEBE especificar un nombre de valor de esquema para que sea preciso en la devolución de resultados.
    - Buenos ejemplos:

```
SELECT ename FROM scott.emp
select EMPNUMBER from SYSTEM.EMP where EMPNUMBER in(5555,4444)
select DNAME from SCOTT.DEPT where DNAME like 'A%G'
SELECT ZIP from SCOTT.FOO where ZIP in (SELECT ZIP FROM SCOTT.FOO)
```

13. En el campo Comparar con valores en grupo, opcionalmente, seleccione un grupo. El grupo seleccionado se utilizará como grupo de valores para buscar en las tablas y/o columnas seleccionadas. Siempre que uno de los valores de un grupo, que sea público o clasificador, coincida, la regla de valor devolverá datos.
14. Marque el recuadro de selección Mostrar valores exclusivos para añadir, a los comentarios, detalles sobre que valores coinciden con las reglas de política de clasificación y se activan. Utilice expresiones regulares en el campo Máscara de valores exclusivos para ocultar los valores exclusivos. Por ejemplo, marque el recuadro de selección Valores exclusivos y utilice ([0-9]{2}-[0-9]{3})-[0-9]{4} en el campo Máscara de valores exclusivos para registrar los últimos cuatro dígitos y ocultar los dígitos de prefijo.

Definir una regla Buscar datos no estructurados

Acerca de esta tarea

Una regla Buscar datos no estructurados examina un archivo que no es de base de datos.

Procedimiento

1. En el recuadro Búsqueda con like, opcionalmente, especifique un valor específico o un patrón basado en comodines. Si se omite, se seleccionarán todos los valores.
2. En el recuadro Expresión de búsqueda, opcionalmente, especifique una expresión regular para definir un patrón para que coincida. Para probar una expresión regular, pulse el icono RE para abrir el panel Crear expresión regular en una ventana separada. Para obtener información detallada sobre cómo utilizar expresiones regulares, consulte Expresiones regulares.
3. Opcionalmente, especifique un nombre de marcador.

Cómo trabajar con acciones de regla de clasificación

Procedimiento

1. Después de guardar una regla, pulse el botón (Personalizar) de esa regla para volver al panel de definición de reglas, desde el que puede añadir una o más acciones de regla.
2. Pulse el botón Nueva acción para abrir el panel Acción.
3. Especifique un nombre de acción.
4. Opcionalmente, especifique una descripción.
5. Seleccione un tipo de acción de la lista. En función de la acción seleccionada, aparecerá un conjunto de campos diferente en el panel.
    - Para las acciones Ignorar y Registrar resultado, no se necesita información adicional.
        - Ignorar: No registrar la coincidencia y no realizar acciones adicionales.
        - Registrar resultado: Registrar la coincidencia y no realizar acciones adicionales.
    - Para todas las demás acciones, aparecerán campos adicionales en el panel y deberá especificar información adicional.
        - Acción Añadir a grupo de objetos/campos
        - Acción Añadir a grupo de objetos
        - Acción Crear regla de acceso
        - Acción Crear conjunto de privacidad
        - Acción Registrar infracción de política
        - Acción Enviar alerta
6. Después de añadir acciones al panel de regla de clasificación, se pueden utilizar los controles de la tabla para modificar las acciones definidas.
7. Pulse Aceptar cuando haya terminado de trabajar con la definición de regla.

Tema principal: Clasificación

Acción Añadir al grupo de objetos/campos

Acerca de esta tarea

Cada vez que la regla de clasificación coincida, se añadirá un miembro al grupo de objetos/campos en el sistema de Guardium. Puede reemplazar todos los miembros o añadir miembros nuevos.

Para un archivo de bases de datos, el componente de objeto del miembro será el nombre de la tabla de base de datos y el componente de campo será el nombre de la columna.

Para un archivo de datos no estructurado, el componente de objeto del miembro será el nombre de archivo (entre comillas) y el componente de campo será el nombre de la columna, pero si no se pueden determinar los nombres de columna, las columnas se denominarán columna1, columna2, etc.

Procedimiento

1. Realice una de las siguientes acciones:
    - Seleccione un grupo de objetos/campos de la lista o
    - Pulse el botón Grupos, defina un grupo nuevo utilizando el Creador de grupos y seleccione ese grupo en la lista.
2. Opcionalmente, marque el recuadro Reemplazar contenido de grupo para reemplazar por completo los miembros del grupo seleccionado con los miembros devueltos por esta regla. De forma predeterminada, este recuadro no está marcado, lo que significa que se añadirán nuevos miembros al grupo pero no se suprimirán miembros. Para un trabajo que se ejecuta a petición, este recuadro se ignora y se le da la oportunidad de añadir o reemplazar miembros en el panel Ver resultados.
3. Pulse el botón Guardar para añadir la acción a la definición de regla, cierre el panel Acción y vuelva al panel de definición de regla.

Acción Añadir a grupo de objetos

Acerca de esta tarea

Cada vez que la regla de clasificación coincida, se añadirá un miembro al grupo de objetos en el sistema de Guardium.

Para un tipo de archivo de bases de datos, el nombre del miembro será el nombre de la tabla de base de datos. Para un tipo de archivo no estructurado, el nombre del miembro será el nombre del archivo.

Puede reemplazar todas las entradas o añadir solo entradas nuevas.

Procedimiento

1. Realice una de las siguientes acciones:
    - Seleccione un grupo objetos de la lista o
    - Pulse el botón Grupos, defina un grupo nuevo utilizando el Creador de grupos y seleccione ese grupo en la lista.
      Nota: Para utilizar alias con grupos generados desde el Clasificador: Abra el Creador de grupos, seleccione el grupo de objetos generado por el clasificador y pulse Modificar. Pulse en el botón Alias en el botón Grupo para cambiar el nombre del grupo de objetos.
2. Opcionalmente, marque el recuadro Reemplazar contenido de grupo para reemplazar por completo los miembros del grupo seleccionado con los miembros devueltos por esta regla. De forma predeterminada, este recuadro no está marcado, lo que significa que se añadirán nuevos miembros al grupo pero no se suprimirán miembros. Para un trabajo que se ejecuta a petición, este recuadro se ignora y se le da la oportunidad de añadir o reemplazar miembros en el panel Ver resultados.
3. Desde el Contenido de miembro real, seleccione el convenio de denominación que se utilizará al añadir el miembro al grupo donde 'Completa' es el schema.tablename y 'Nombre' es el tablename.
4. Pulse Guardar para añadir la acción a la definición de regla, cierre el panel Acción y vuelva al panel de definición de regla.

Acción Crear regla de acceso

Acerca de esta tarea

Cada vez que la regla de clasificación coincida, se insertará una regla de acceso en una definición de política de seguridad existente. La política de seguridad actualizada no se instalará (esta tarea se realiza de forma separada, normalmente la realiza un administrador de Guardium).

Procedimiento

1. Seleccione una Política de acceso de la lista. Debe estar autorizado para acceder a esta política.
2. Especifique un nombre de regla en el recuadro Descripción de regla.
3. Seleccione una acción en la lista Acción de regla de acceso.
4. Opcionalmente, seleccione un Grupo de mandatos o pulse el botón Grupos, defina un nuevo Grupo de mandatos utilizando el Creador de grupos y seleccione ese Grupo de mandatos en la lista.
5. Para registrar valores de campo por separado, marque el recuadro de selección Incluir campo. De lo contrario, solo se registrará la tabla (la predeterminada).
6. Para incluir la dirección IP del servidor, marque el recuadro de selección Incluir IP de servidor.
7. Si ha seleccionado una acción de alerta, aparece una fila de Receptor en el panel y debe añadir como mínimo un receptor para la alerta. Pulse Modificar receptores para añadir uno o más receptores.
8. Pulse Aceptar para añadir la acción a la definición de regla, cierre el panel Acción y vuelva al panel de definición de regla.

Acción Crear conjunto de privacidad

Acerca de esta tarea

Cada vez que la regla de clasificación coincida, se reemplazará la lista de campos/objetos del conjunto de privacidad seleccionado.

Para un archivo de bases de datos, el componente de objeto del conjunto de privacidad será el nombre de la tabla de base de datos y el componente de campo será el nombre de la columna.

Para un archivo de datos no estructurado, el componente de objeto del conjunto de privacidad será el nombre de archivo (entre comillas) y el componente de campo será el nombre de la columna, pero si no se pueden determinar los nombres de columna, las columnas se denominarán columna1, columna2, etc.

Procedimiento

1. Seleccione el Conjunto de privacidad cuyos contenidos desee reemplazar.
2. Pulse el botón Aceptar para añadir la acción a la definición de regla, cierre el panel Acción y vuelva al panel de definición de regla.

Acción Registrar infracción de política

Acerca de esta tarea

Cada vez que la regla de clasificación coincida, se registrará una infracción de política. Esto significa que las infracciones de políticas de clasificación se registrarán (y se pueden informar) junto con las infracciones de políticas de acceso (y, opcionalmente, alertas de correlación) que se puedan haber producido.

Procedimiento

1. Seleccione un código de gravedad de la lista.
2. Pulse el botón Aceptar para añadir la acción a la definición de regla, cierre el panel Acción y vuelva al panel de definición de regla.

Acción Enviar alerta

Acerca de esta tarea

Pulse el botón Aceptar para añadir la acción a la definición de regla, cierre el panel Acción y vuelva al panel de definición de regla.

Procedimiento

1. Seleccione un código de tipo de notificación de la lista.
2. Pulse el botón Modificar receptores para añadir uno o más receptores. El receptor especificado recibirá un correo electrónico por origen de datos, por regla y por acción. Por lo tanto, si un origen de datos tiene tres reglas y cada una tiene dos acciones (que tienen por lo menos una coincidencia), el usuario recibirá 2 * 3 = 6 correos electrónicos.
3. Pulse el botón Aceptar para añadir la acción a la definición de regla, cierre el panel Acción y vuelva al panel de definición de regla.

Descubrir datos confidenciales

Cree un escenario integral para descubrir y clasificar datos confidenciales.

Acerca de esta tarea

Los procesos de descubrimiento y clasificación se vuelven importantes a medida que el tamaño de la organización crece y la información confidencial como, por ejemplo, los números de tarjeta de crédito y datos financieros personales se propagan en varias ubicaciones. Esto sucede a menudo en el contexto de las fusiones y las adquisiciones o cuando los sistemas existentes han durado más que los propietarios originales. Como resultado, es posible que existan datos confidenciales más allá del conocimiento de la persona que actualmente es propietaria de esos datos. Se trata de un escenario común pero extremadamente vulnerable, puesto que no puede proteger los datos confidenciales a menos que sepa que existen.

Los escenarios de descubrimiento de datos confidenciales abarcan tres aspectos críticos de la seguridad empresarial:

- Descubrimiento: Ubicación de los datos confidenciales que existen en cualquier lugar de su entorno.
- Protección: Supervisión y alertas cuando se accede a los datos confidenciales.
- Cumplimiento: Creación de seguimientos de auditoría para revisar los resultados de los procesos de descubrimiento de datos confidenciales.

El creador de escenarios integrales Descubrir datos confidenciales agiliza los procesos de descubrimiento, protección y cumplimiento integrando varias herramientas de Guardium en una única interfaz sencilla.

Tabla 1. Correlación de herramientas de descubrimiento de datos confidenciales.

Valor	Tarea de escenario	Descripción	Resultado
Descubrir	Nombre y descripción	Proporciona un nombre y una descripción para el escenario y las políticas y procesos relacionados.	Crea un proceso de clasificación y una política de clasificación. Opcionalmente, crea nuevas definiciones de origen de datos.
	Qué se va a descubrir	Crea reglas y acciones de regla para descubrir y clasificar datos.	
	Área de búsqueda	Identifica los orígenes de datos a escanear.	
	Ejecutar descubrimiento	Ejecuta el escenario, revisa los resultados y define acciones de alertas y agrupación ad hoc.	
Proteger	Revisar informe		Crea una política de acceso.
Cumplir	Auditoría	Define los destinatarios, una secuencia de distribución y opciones de revisión.	Crea un proceso de auditoría.
	Planificación	Crea una planificación para ejecutarse en intervalos definidos.	

Esta secuencia de tareas le guía a través de los procesos de creación de un nuevo escenario de descubrimiento. Esto incluye la creación de *políticas de clasificación* que consisten en reglas y acciones de regla para el descubrimiento de datos confidenciales, la creación de *procesos de clasificación* identificando orígenes de datos en los que escanear en busca de datos confidenciales, la definición de políticas ad hoc (por ejemplo, para agrupación y alertas) y la creación de *procesos de auditoría* que distribuyen resultados a diferentes interesados en intervalos planificados.

Mientras que un escenario de descubrimiento de datos confidenciales crea políticas y procesos subyacentes a los que se puede acceder utilizando otras herramientas de Guardium (por ejemplo, el Creador de políticas de clasificación o mediante mandatos GuardAPI), no hay mandatos GuardAPI para crear o modificar un escenario de descubrimiento.

1. Escenario de descubrimiento
   Crear un nuevo escenario de descubrimiento o seleccionar uno existente para copiarlo o editarlo.
2. Nombre y descripción
   Proporciona un nombre y una descripción para su escenario de descubrimiento.
3. Qué se va a descubrir
   Crear políticas formadas por reglas y acciones de reglas para descubrir y clasificar datos confidenciales.
4. Área de búsqueda
   Identificar los orígenes de datos a escanear en busca de datos confidenciales.
5. Ejecutar descubrimiento y revisar informe
   Opcionalmente, ejecute el escenario de descubrimiento y revise los resultados.
6. Auditoría
   Opcionalmente, crear un proceso de auditoría definiendo receptores, una secuencia de distribución y opciones de revisión para el informe de descubrimiento y clasificación.
7. Planificación
   Opcionalmente, active el proceso de auditoría planificándolo para que se ejecute en los intervalos definidos.

Qué hacer a continuación

Continúe en la sección siguiente y proporcione un Nombre y descripción para su escenario de descubrimiento y clasificación.
Tema principal: Descubrir

Escenario de descubrimiento

Crear un nuevo escenario de descubrimiento o seleccionar uno existente para copiarlo o editarlo.

Procedimiento

1. Navegue a Descubrir > Escenarios integrales > Descubrir datos confidenciales.
2. Cree, copie o edite un escenario de descubrimiento.
   - Pulse el icono para crear un nuevo escenario.
   - Pulse el icono para copiar un escenario existente o plantilla.
   - Pulse el nombre de un escenario existente en la lista de Escenarios de descubrimiento para empezar a editar ese escenario.

   Algunos escenarios de descubrimiento o plantillas vienen proporcionadas de forma predeterminada, incluyendo los siguientes:

   GDPR [plantilla]
   : El escenario GDPR [plantilla] proporciona el último conjunto de reglas de descubrimiento y soporte de idioma para su estrategia de cumplimiento GDPR. Las plantillas se pueden copiar o editar y guardar con otro nombre y GDPR [plantilla] siempre recibirá las últimas reglas de descubrimiento GDPR y soporte de idioma.

   GDPR
   : El escenario GDPR proporciona un conjunto básico de reglas de descubrimiento que puede utilizarse como parte de una estrategia de cumplimiento GDPR. Puede editar y guardar cambios en el escenario GDPR, pero el escenario no recibirá reglas actualizadas ni soporte de idioma a lo largo del tiempo.
     Atención: Si GDPR [plantilla] está disponible, no se recomienda utilizar el escenario GDPR anterior porque el escenario GDPR no recibe actualizaciones.

Tema principal: Descubrir datos confidenciales
Tema siguiente: Nombre y descripción

Nombre y descripción

Proporciona un nombre y una descripción para su escenario de descubrimiento.

Acerca de esta tarea

El nombre proporcionado para el escenario de descubrimiento también se utilizará para nombrar las políticas y procesos subyacentes.

Durante este paso, también puede especificar los *roles de seguridad* que pueden acceder al escenario de descubrimiento.

Procedimiento

1. Abra la sección Nombre y descripción y proporcione o edite el nombre y la descripción (opcional) del escenario. El nombre que proporcione aquí también se utilizará para nombrar los procesos de clasificación y las políticas subyacentes creadas por el escenario de descubrimiento.
   Ejemplo: Un escenario de descubrimiento llamado "Find PCI" creará un *proceso de clasificación* llamado "Find PCI" y una *política de clasificación* llamada "Find PCI Classification Policy" (seguido de una indicación de fecha y hora).
2. Proporcione la categoría y las etiquetas de clasificación para etiquetar infracciones. "Confidencial" es el valor predeterminado para las etiquetas de categoría y clasificación.
3. Opcionalmente, pulse el botón Roles para especificar los *roles de seguridad* que pueden acceder al escenario de descubrimiento.

Qué hacer a continuación

Continúe en la siguiente sección del escenario de descubrimiento, Qué se va a descubrir.
Tema principal: Descubrir datos confidenciales
Tema anterior: Escenario de descubrimiento
Tema siguiente: Qué se va a descubrir

Qué se va a descubrir

Crear políticas formadas por reglas y acciones de reglas para descubrir y clasificar datos confidenciales.

Acerca de esta tarea

Las *políticas de clasificación* contienen conjuntos de reglas y acciones de reglas ordenados que identifican y realizan acciones en datos confidenciales. Cada regla en una política define una acción condicional que se toma cuando se cumple la regla. La prueba condicional puede ser simple, por ejemplo, una serie comodín encontrada en cualquier parte de una tabla, o una prueba compleja que tenga en cuenta varias condiciones. Para escenarios de descubrimiento de datos confidenciales, la acción desencadenada por una regla puede ser una acción de agrupación que añada el objeto a un grupo especificado o una acción de alerta que desencadene una notificación cuando coincidan las reglas. Se pueden combinar y ordenar varias acciones de agrupación y alerta para crear respuestas sofisticadas a reglas coincidentes.

Esta tarea le guía a través de los procesos de creación y edición de reglas de clasificación y acciones de regla para utilizarlas en su escenario de descubrimiento.

Procedimiento

1. Abra la sección Qué se va a descubrir para definir reglas para el descubrimiento de datos.
2. Utilice el menú Idioma para filtrar plantillas de reglas según el idioma seleccionado y los países donde el idioma seleccionado es un idioma oficial. Las plantillas para patrones universales como, por ejemplo, números de tarjetas de crédito y direcciones de correo electrónico se visualizan para todas las selecciones del menú Idioma.
3. Añada reglas a su escenario de descubrimiento realizando una de las acciones siguientes:
   - Pulse el icono para crear una nueva regla.
   - Seleccione las reglas de la tabla Plantillas de reglas de clasificación y pulse el icono para añadir reglas predefinidas.
4. Defina una nueva regla o edite una plantilla de regla seleccionando la plantilla y pulsando el icono .
   a. Seleccione un Tipo de regla basado en el tipo de búsqueda que se está realizando.
      - Buscar datos: Compara patrones específicos o valores en los datos.
      - Búsqueda de catálogo: Compara nombres de tabla o columna en el catálogo de bases de datos.
      - Búsqueda de datos no estructurados: Compara valores específicos o patrones en un archivo de datos no estructurado, por ejemplo archivos CSV, TXT, o CEF.
   b. Proporcione un nombre y una descripción mientras, opcionalmente, especifica una *prueba de patrón especial* al principio del campo Nombre. El nombre de regla también se utilizará para nombrar la regla asociada con la política de clasificación en el Creador de políticas de clasificación. Si necesita una prueba de patrón especial, se recomienda que trabaje con la plantilla correspondiente (por ejemplo, utilice Tarjeta bancaria: Número de tarjeta de crédito para números de tarjeta de crédito).
   c. Abra la sección Criterio de regla para definir una *expresión regular* y otros criterios de búsqueda para la regla. Si está trabajando con una plantilla, se proporciona una *expresión regular* adecuada de forma predeterminada.
   Atención: Para las reglas creadas en el escenario de descubrimiento de datos confidenciales, el Tipo de datos predeterminado incluye tanto Número como Texto.
   d. Abra la sección Acciones y defina las *acciones de regla* que se deben realizar cuando los criterios de regla coincidan.
   e. Al definir varias *acciones de regla* opcionalmente, puede pulsar el icono y utilizar los iconos y para cambiar el orden en que se ejecutan las acciones.
   f. Pulse Guardar cuando haya terminado de añadir o editar definiciones de reglas para volver a la sección Qué se va a descubrir del escenario de descubrimiento.
5. Opcionalmente, pulse el icono y utilice los iconos y para cambiar el orden en que se aplican las reglas. El orden de las reglas es importante ya que el comportamiento predeterminado detiene la ejecución tras la primera coincidencia a menos que se seleccione Continuar en coincidencia en los Criterios de regla.
6. Cuando haya terminado de trabajar con las reglas, pulse Siguiente para empezar a trabajar en la siguiente sección del escenario de descubrimiento.

Qué hacer a continuación

Continúe en la siguiente sección del escenario de descubrimiento, Área de búsqueda.
Tema principal: Descubrir datos confidenciales
Tema anterior: Nombre y descripción
Tema siguiente: Área de búsqueda
Conceptos relacionados:

Expresiones regulares
Tareas relacionadas:
Cómo trabajar con acciones de regla de clasificación
Referencia relacionada:
Contenido de miembro real
Criterio de regla
Pruebas de patrones especiales

Criterio de regla

Tabla 1.

Atributo	Descripción
Tipo de tabla	Seleccione uno o más tipos de tabla para buscar: Sinónimo, Tabla, o Ver. La tabla está seleccionada de forma predeterminada.
Tipo de datos	Seleccione uno o más tipos de datos para buscar: Número, Texto o Fecha. Número y Texto están seleccionados de forma predeterminada.
Expresión de búsqueda	Opcionalmente, especifique una expresión regular para definir un patrón de búsqueda que coincida. Para probar una expresión regular, pulse el botón RE para abrir el editor de expresiones regulares.
Nombre de tabla como	Opcionalmente, especifique un nombre específico o un patrón de caracteres comodín. Si se omite, se seleccionan todos los nombres de tabla.
Nombre de columna como	Opcionalmente, especifique un nombre específico o un patrón de caracteres comodín. Si se omite, se seleccionan todos los nombres de columna.
Continuar en coincidencia	Si la siguiente regla en la política de clasificación debe evaluarse después de que coincida, marque el recuadro de selección Continuar en coincidencia. De forma predeterminada, se dejan de evaluar las reglas una vez que la regla coincide.
Comodín de búsqueda	Opcionalmente, especifique un valor específico o un patrón comodín. Si se omite, se seleccionan todos los valores.
Longitud mínima	Opcionalmente, especifique la longitud mínima. Si se omite, no hay límite.
Longitud máxima	Opcionalmente, especifique la longitud máxima. Si se omite, no hay límite.
Nombre de evaluación	Opcionalmente, especifique un nombre de clase Java™ completo que haya sido creado y subido. A continuación, se utilizará la clase Java para activar y evaluar la serie. Nota: No hay ninguna validación de que el nombre de clase especificado se haya cargado y se ajuste a la interfaz.
Marcador Activar solo con	El marcador Activar solo con permite la agrupación de tipos reglas de clasificación: Reglas con la misma activación del marcador al mismo tiempo. Además, todas las reglas devueltas que utilizan un marcador deben devolver datos basados en el mismo nombre de tabla. Si se definen dos o más reglas con el mismo marcador, estas reglas se activarán conjuntamente de modo que si se activan en la misma tabla, ambas se registrarán y se invocarán sus acciones. Por el contrario, si solo una de ellas se activa en una tabla, ninguna de las reglas se registrará o se invocarás sus acciones. Ser capaz de poder activar varias reglas conjuntamente se vuelve importante cuando se ocupa de datos confidenciales que aparecen juntos en la misma tabla. Por ejemplo, es posible que desee saber cuándo una tabla tiene un número de seguridad social y un carnet de conducir de Massachusetts. El marcador Activar solo con es un valor constante, se puede elegir cualquier valor y debe tener exactamente el mismo valor en todas las reglas que desea agrupar. Esto significa que si una regla tiene un marcador ABC, la otra regla con la que desea agruparla debe tener también un marcador denominado ABC. El marcador Activar solo con también interactúa con el distintivo Continuar en coincidencia. Por ejemplo, si se han definido las reglas de forma que la Regla 3 no coincida con el Continuar en coincidencia no se devolverán resultados a pesar de que las tres reglas de marcador fueran positivas. Esto se debe a que no se ha podido ejecutar la Regla 4 y no se activará la agrupación porque todos los marcadores Activar solo con deben ejecutarse con resultados positivos. Regla 1. Regla de marcador de activación "ABC" (Continuar en coincidencia). Regla 2. Regla de marcador de activación "ABC" (Continuar en coincidencia). Regla 3. Tipo de regla de no marcador de activación (Continuar en coincidencia) Regla 4. Regla de marcador de activación "ABC" (Continuar en coincidencia).
Porcentaje de aciertos	Opcionalmente, especifique un porcentaje de datos coincidentes que se deba conseguir para que se active esta regla. Se devuelven los datos si el porcentaje de datos coincidentes examinado es mayor o igual (>=) que el valor de porcentaje especificado, tenga en cuenta que una entrada vacía significa que no hay una condición y no afectará si la regla se activa o no y devuelve datos a la pantalla de la vista. Un porcentaje de 0 hará que la regla se active para esta condición y devuelva datos a la pantalla de la vista y un porcentaje de 100 requiere que todo coincida.

Comparar con valores en SQL	Opcionalmente, especifique una sentencia SQL. El SQL especificado, que debe estar basado en la información de retorno de una sola columna, se utilizará como grupo de valores para buscar en las tablas y columnas seleccionadas.
	Nota: Si se utiliza, Comparar con valores en SQL debería observar las siguientes reglas:
	
	• La sentencia SQL DEBE empezar con `SELECT`.
	• La sentencia SQL NO DEBE utilizar `;` (punto y coma).
	• El SQL especificado DEBE especificar un nombre de valor de esquema para que sea preciso en la devolución de resultados.
	
	• Buenos ejemplos:
	
	`SELECT ename FROM scott.emp`
	`select EMPNUMBER from SYSTEM.EMP where EMPNUMBER in(5555,4444)`
	`select DNAME from SCOTT.DEPT where DNAME like 'A%G'`
	`SELECT ZIP from SCOTT.FOO where ZIP in (SELECT ZIP FROM SCOTT.FOO)`

Comparar con valores en grupo	Opcionalmente, seleccione un grupo. El grupo seleccionado se utilizará como grupo de valores para buscar en las tablas y columnas seleccionadas. Siempre que uno de los valores de un grupo, que sea público o clasificador, coincida, la regla de valor devolverá datos.

Atributo	Descripción
Mostrar valores exclusivos	Marque el recuadro de selección Mostrar valores exclusivos para añadir detalles sobre que valores coinciden con las reglas de política de clasificación en los campos de comentarios del informe de resultados.
Máscara de valores exclusivos	Utilice expresiones regulares en el campo Máscara de valores exclusivos para ocultar los valores exclusivos. Por ejemplo, marque el recuadro de selección Mostrar valores exclusivos y utilice `([0-9]{2}-[0-9]{3})-[0-9]{4}` en el campo Máscara de valores exclusivos para registrar los últimos cuatro dígitos y ocultar los dígitos de prefijo.

Tema principal: Qué se va a descubrir

Contenido de miembro real

Utilice el campo Contenido de miembro real para definir cómo la acción de regla Añadir a grupo de objetos etiqueta los objetos.

Tabla 1.

Selección de Contenido de miembro real	Valor en grupo
Solo nombre de objeto	tableName
Like Name%	tableName%
Like %Name	%tableName
Like %Name%	%tableName%
%/%.Name	%%.tableName
Nombre completo	schemaName.tableName
Like Full%	schemaName.tableName%
Like %Full	%schemaName.tableName
Like %Full%	%schemaName.tableName%
%/Full	%%.schemaName.tableName
Read/%.Name	Read/%.tableName
Change/%.Name	Change/%.tableName
Read/Full	Read/schemaName.tableName
Change/Full	Change/schemaName.tableName

Si sus reglas devuelven el nombre de la tabla `JJ_CREDIT_CARD` del esquema `DB2INST1` y ha especificado una acción Añadir a grupo de objetos, las selecciones de Contenido de miembro real se comportan de la siguiente manera:

- Seleccionando Nombre completo añade `DB2INST1.JJ_CREDIT_CARD` al grupo seleccionado.
- Seleccionando Solo nombre de objeto añade `JJ_CREDIT_CARD` al grupo seleccionado.
- Seleccionando Change/Full añade `Change/DB2INST1.JJ_CREDIT_CARD` al grupo seleccionado.

Tema principal: Qué se va a descubrir

Área de búsqueda

Identificar los orígenes de datos a escanear en busca de datos confidenciales.

Acerca de esta tarea

Los orígenes de datos almacenan información sobre la base de datos o el repositorio como, por ejemplo, el tipo de base de datos, la ubicación del repositorio o las credenciales de autenticación que se pueden asociar con el mismo. Añadir orígenes de datos a un escenario de descubrimiento crea un *proceso de clasificación* donde las *políticas de clasificación* se aplican en los orígenes de datos seleccionados.

En esta tarea, identifique los orígenes de datos en los que desea buscar datos confidenciales.

Procedimiento

1. Abra la sección Área de búsqueda para identificar los orígenes de datos en los que desea buscar datos confidenciales.
2. Añada orígenes de datos a su escenario de descubrimiento realizando una de las acciones siguientes:
   - Pulse el icono para abrir el diálogo Crear origen de datos y añada una nueva definición de origen de datos.
   - Seleccione orígenes de datos de la tabla Orígenes de datos disponibles y pulse el icono para añadir orígenes de datos existentes.
3. Defina un nuevo origen de datos o edite un origen de datos existente seleccionándolo y pulsando el icono . Los nuevos orígenes de datos definidos a través del escenario de descubrimiento también pueden visualizarse o editarse mediante la herramienta Definiciones de orígenes de datos.
   a. Proporcione o edite el nombre del origen de datos.
   b. Seleccione el tipo de base de datos adecuado en el menú Tipo de base de datos y proporcione la información solicitada para completar la definición de origen de datos. Los campos disponibles difieren en función del tipo de base de datos seleccionado.
   c. Cuando haya terminado de editar la definición del origen de datos, pulse Guardar para guardar su trabajo y, opcionalmente, pulse Probar conexión para verificar la conexión del origen de datos.
   d. Cuando haya terminado de trabajar con la definición de origen de datos, pulse Cerrar para cerrar el diálogo.
4. Si también está utilizando este proceso de clasificación para bases de datos en la nube, seleccione Habilitar la auditoría de objetos para bases de datos en la nube.
5. Cuando haya terminado de añadir orígenes de datos, pulse Siguiente para empezar a trabajar en la siguiente sección del flujo de trabajo de descubrimiento.

Resultados

Se crea un *proceso de clasificación* después de añadir orígenes de datos a su escenario de descubrimiento y guardar el escenario. Para ver o editar este proceso directamente, utilice el Creador de procesos de clasificación.

Qué hacer a continuación

Continúe en la siguiente sección del flujo de trabajo de descubrimiento, Ejecutar descubrimiento.
Tema principal: Descubrir datos confidenciales
Tema anterior: Qué se va a descubrir
Tema siguiente: Ejecutar descubrimiento y revisar informe
Conceptos relacionados:
Orígenes de datos
Tareas relacionadas:
Creación de una definición de origen de datos

Ejecutar descubrimiento y revisar informe

Opcionalmente, ejecute el escenario de descubrimiento y revise los resultados.

Acerca de esta tarea

Después de definir las políticas para descubrir datos confidenciales e identificar orígenes de datos en los que buscar, puede ejecutar el *Proceso de clasificación* y revisar los resultados. Ejecutar el proceso y revisar los resultados le permite ajustar las políticas, por ejemplo, especificando criterios de búsqueda adicionales si encuentra que los resultados son demasiado amplios. Es posible que tenga que pasar por varias interacciones de refinado de políticas, ejecución del proceso y evaluación de los resultados antes de alcanzar los resultados deseados.

Procedimiento

1. Abra la sección Ejecutar descubrimiento para probar su escenario de descubrimiento.
2. Pulse Ejecutar ahora para empezar.
   Atención:
   - En función de las políticas que haya especificado y la cantidad de orígenes de datos que haya seleccionado para buscar, puede tardar varios minutos o más en completar el proceso de identificación de datos confidenciales. El estado del proceso se indica junto al botón Ejecutar ahora o puede supervisar el proceso utilizando la Cola de trabajos de Guardium.
   - También puede ejecutar el *proceso de clasificación* visitando el Creador de procesos de clasificación, seleccionando su *proceso de clasificación* y pulsando en Ejecutar una vez ahora.
3. Cuando haya finalizado la ejecución del escenario de descubrimiento, abra la sección Revisar informe para ver los resultados.
4. Al revisar los resultados, puede definir reglas y acciones adicionales en función de los resultados. Utilice el Filtro para acotar los resultados (el filtrado no está soportado con más de 10.000 resultados).
   a. Seleccione las filas que contienen los datos sobre los que desea definir acciones.
   b. Pulse Añadir a grupo para definir una acción de agrupación o pulse en Acciones avanzadas para definir otras acciones como alertas, registro o ignorar.
   c. Después de completar el diálogo para definir una acción, pulse Aceptar para volver al informe de resultados.
      Atención:
      - Las acciones añadidas desde la tabla de resultados se consideran acciones ad hoc que solo se ejecutan si se invocan desde la tabla de resultados. Estas acciones no aparecerán en la sección Qué se va a descubrir > Editar regla > Acciones de su escenario de descubrimiento y no se ejecutarán automáticamente como parte del escenario de descubrimiento o los *procesos de clasificación* relacionados.
      - Utilice el Creador de políticas para revisar, editar e instalar acciones de alerta y reglas de acceso.
      - Utilice el Creador de grupos para revisar y editar las acciones de agrupación.
      - Utilice el Creador de conjuntos de privacidad para revisar acciones de conjuntos de privacidad.
      - Utilice la herramienta de Gestión de incidencias para revisar acciones de registro de políticas.
5. Cuando haya terminado de revisar el informe de resultados, pulse Siguiente para empezar a trabajar en la siguiente sección del escenario de descubrimiento.

Resultados

Después de ejecutar la búsqueda de datos confidenciales, supervise su estado junto al botón Ejecutar ahora o utilizando la Cola de trabajos de Guardium. Puede utilizar el Creador de grupos para revisar cualquier acción de agrupación o el Creador de políticas para revisar e instalar cualquier acción de alertas que se haya añadido desde la tabla de resultados.

Qué hacer a continuación

Opcionalmente, continúe en la siguiente sección del escenario de descubrimiento, Auditoría.
Tema principal: Descubrir datos confidenciales
Tema anterior: Área de búsqueda
Tema siguiente: Auditoría

Auditoría

Opcionalmente, crear un proceso de auditoría definiendo receptores, una secuencia de distribución y opciones de revisión para el informe de descubrimiento y clasificación.

Acerca de esta tarea

Puede definir cualquier número de receptores para los resultados de un flujo de trabajo de descubrimiento y puede controlar el orden en que reciben los resultados. Además, puede especificar opciones de control de procesos, como si un receptor debe aprobar los resultados antes de enviarlos al siguiente receptor.

El *proceso de auditoría* creado mediante la adición de receptores a un escenario de descubrimiento hereda el nombre del escenario. Por ejemplo, añadir receptores a un escenario de descubrimiento llamado "Find PCI" crea un *proceso de auditoría* llamado "Find PCI Audit process" seguido de una indicación de fecha y hora.

Procedimiento

1. Abra la sección Auditoría para definir receptores para informes de descubrimiento.
2. Añada receptores a su escenario de descubrimiento pulsando en el icono y definiendo las opciones de cómo se entregan los informes.
   - Si envía el informe a usuarios, roles o grupos de Guardium, deberá definir opciones de control de procesos.
   - Si envía el informe a receptores de correo electrónico, proporcione sus direcciones de correo electrónico y filtre el informe por el nombre de usuario de Guardium adecuado para el receptor de correo electrónico.
3. Pulse Aceptar para añadir el receptor al flujo de trabajo de descubrimiento. Continúe añadiendo receptores adicionales al escenario si es necesario.
4. Opcionalmente, pulse el icono y utilice los iconos y para cambiar el orden en que se distribuyen los informes a los receptores. Es importante cuando se utiliza la distribución *secuencial* ya que determina que receptor debe revisar o aprobar el informe antes de que se envíe a los receptores siguientes.
5. Cuando haya terminado de añadir, editar y ordenar receptores, pulse Siguiente para empezar a trabajar en la siguiente sección del flujo de trabajo de descubrimiento.

Resultados

Un *proceso de auditoría* se crea después de definir receptores y guardar el escenario de descubrimiento. Para ver, editar o ejecutar este proceso directamente, utilice el Creador de procesos de auditoría.

El *proceso de auditoría* permanece inactivo hasta que se planifica utilizando la sección Planificar del escenario de descubrimiento o el Creador de procesos de auditoría. También puede ejecutar el *proceso de auditoría* visitando el Creador de procesos de auditoría, seleccionando el *proceso de auditoría* y pulsando Ejecutar una vez ahora.

Qué hacer a continuación

Opcionalmente, continúe en la siguiente sección del flujo de trabajo de descubrimiento, Planificar.
Tema principal: Descubrir datos confidenciales
Tema anterior: Ejecutar descubrimiento y revisar informe
Tema siguiente: Planificación
Conceptos relacionados:
Creación de procesos de auditoría

Planificación

Opcionalmente, active el proceso de auditoría planificándolo para que se ejecute en los intervalos definidos.

Acerca de esta tarea

Una planificación pasa a formar parte de un *proceso de auditoría* junto con cualquier receptor especificado en la sección Auditoría del escenario de descubrimiento. La definición de una planificación ejecuta el *proceso de auditoría* en los intervalos especificados y garantiza que los resultados del *proceso de clasificación* asociados se distribuyen y revisan de forma regular.

Procedimiento

1. Abra la sección Planificación para definir una planificación para el descubrimiento de datos.
2. Utilice el menú Planificar por para definir intervalos diarios o mensuales para el *proceso de auditoría*.
3. Utilice los recuadros de selección Iniciar planificación cada y Repetir cada para definir cuantas veces al día y cuantas veces a la hora se ejecuta el *proceso de auditoría*.
4. Utilice los controles de Fecha y hora de inicio para definir una fecha y hora explícita para el inicio de la planificación.
5. Desmarque el recuadro de selección Activar planificación para desactivar el *proceso de auditoría* mientras se retiene la información de planificación para su uso posterior. El recuadro de selección Activar planificación está marcado de forma predeterminada, lo que significa que el proceso de auditoría pasa a estar activo después de guardar la planificación.
6. Cuando haya definido una planificación, pulse Guardar para finalizar la edición y cerrar el editor de flujos de trabajo.

Resultados

Se crea un *proceso de auditoría* después de definir una planificación y guardar el escenario de descubrimiento. Para ver o editar este proceso de auditoría directamente, utilice el Creador de procesos de auditoría. Revise el informe Trabajos planificados para ver el estado, la fecha de inicio y la siguiente hora de activación de las tareas de auditoría planificadas.
Tema principal: Descubrir datos confidenciales
Tema anterior: Auditoría
Conceptos relacionados:
Creación de procesos de auditoría

Expresiones regulares

Se pueden utilizar expresiones regulares para buscar tráfico de patrones complejos en los datos.

La implementación de IBM Guardium de expresiones regulares es compatible con POSIX 1003.2. Para obtener información más detallada, consulte el sitio web de Open Group: www.opengroup.org. Se pueden utilizar expresiones regulares para buscar tráfico de patrones complejos en los datos. Consulte las políticas para obtener ejemplos.

Este tema de ayuda proporciona instrucciones para el uso de la herramienta Crear expresión regular y varias tablas de caracteres y construcciones especiales utilizadas habitualmente. No proporciona una descripción exhaustiva de cómo se construyen o utilizan las expresiones regulares. Consulte el sitio web de Open Group para obtener información más detallada.

El punto importante a tener en cuenta sobre la coincidencia de patrones o de XML utilizando expresiones regulares es que la búsqueda de una coincidencia empieza en el principio de una serie y de detiene cuando se encuentra la primera secuencia coincide con la expresión. Se pueden utilizar diferentes o las mismas expresiones regulares para la coincidencia de patrones y de XML al mismo tiempo.

Nota: IBM Guardium no soporta expresiones regulares para idiomas que no sean el inglés.

Utilización de la herramienta Crear expresión regular

Cuando un campo de entrada necesita una expresión regular, puede utilizar la herramienta Crear expresión regular para codificar y probar una expresión regular. El icono Crear expresión regular se encuentra en el Creador de políticas bajo Añadir regla.

Para abrir la herramienta Crear expresión regular, pulse el icono RE junto al campo que contendrá la expresión regular. Si ya ha especificado algo en el campo, se copiará en el recuadro de expresión regular del panel Crear expresión regular.

1. Seleccione una categoría de expresiones regulares en la lista desplegable.
2. Seleccione un patrón de la lista desplegable.
3. Especifique o modifique la expresión en el recuadro de expresión regular.
4. Para probar la expresión, especifique un texto en el recuadro Texto para la coincidencia y pulse el botón Probar:
   - Si la expresión contiene un error (por ejemplo, si falta una llave de cierre), se le informará con un mensaje de Error de sintaxis.
   - El mensaje Coincidencia encontrada indica que su expresión regular ha encontrado una coincidencia en el texto que ha especificado.
   - Si no se encuentra ninguna coincidencia, se visualiza el mensaje `No se ha encontrado ninguna coincidencia`.
5. Le sugerimos que repita el paso varias veces para verificar que su expresión regular coincide y no coincide como se espera para su propósito.
6. Parar especificar un carácter especial al final de su expresión regular, puede seleccionarlo en la lista Seleccionar elemento. Para especificar un carácter especial en cualquier otro lugar, debe escribirlo o copiarlo.
7. Cuando acabe de realizar cambios y pruebas, pulse Aceptar para cerrar el panel Crear expresión regular y copie la expresión regular en el panel de definición.

Caracteres especiales y construcciones

La siguiente tabla proporciona un resumen de los caracteres especiales y construcciones utilizadas con más frecuencia.

Tabla 1. Caracteres especiales y construcciones

Carácter	¿Cómo se hace para...?	Ejemplo	Coincidencias	No hay coincidencia
literal	Coincidir con una secuencia de caracteres exacta (sensible a las mayúsculas y minúsculas), excepto por los caracteres especiales descritos a continuación.	can	can	Can cab caN
. (punto)	Coincidir con cualquier carácter incluidos los caracteres de retorno o de nueva línea (\n).	ca.	can cab	c cb
*	Coincidir cero o más veces con el carácter o caracteres anteriores.	Ca*n	Cn Can Caan	Cb Cabn
^	Coincidir con el principio de la serie con los siguientes caracteres.	^C.	Ca	ca a
$	Coincidir con el final de la serie con los caracteres anteriores.	C.n$	Can Cn	Cab
+	Coincidir una o más veces con los caracteres anteriores.	^Ca+n	Can Caan	Cn
?	Coincidir cero o una vez con los caracteres anteriores.	Ca?n	Cn Can	Caan
|	Coincidir con el patrón siguiente o el anterior.	Can|cab	Can cab	Cab
(x ...)	Coincidir con la secuencia entre paréntesis.	(Ca)*n	Can XaCan	Cn CCnn
{n}	Coincidir exactamente n veces con los caracteres anteriores.	Ca{3}n	Caaan	Caan Caaaan
{n,}	Coincidir n o más veces con los caracteres anteriores.	Ca{2,}n	Caan Caaaan	Can Cn
{n,m}	Coincidir entre n y m veces con los caracteres anteriores.	Ca{2,3}n	Caan Caaan	Can Caaaan
[a-ce]	Coincidir con un único carácter del conjunto, donde el guion indica una secuencia contigua. Por ejemplo, [0-9] coincide con cualquier número.	[C-FL]an	Can Dan Lan	Ban
[^a-ce]	Coincidir con cualquier carácter que NO esté en el conjunto especificado.	[^C-FL]an	aan Ban	Can Dan
[[.char.]]	Coincidir con el carácter especificado o el nombre del carácter de la tabla de caracteres con nombres.	[[.~.]]an o [[.tilde.]]an	~an	@an
[[:class:]]	Coincidir con cualquier carácter en la clase de caracteres especificada, de la tabla de clases de caracteres.	[[:alpha:]]+	abc	ab3

Tabla de caracteres con nombres (Inglés)

La siguiente tabla describe los nombres de caracteres estándar que pueden utilizarse dentro de los paréntesis en las expresiones regulares ([[.char]]). Los nombres de caracteres son específicos de ubicación, de modo que las versiones no inglesas de Guardium pueden utilizar un conjunto de nombres de caracteres distinto.

- NUL \0
- SOH \001
- STX \002
- ETX \003
- EOT \004
- ENQ \005
- ACK \006
- BEL \007
- alerta \007

- BS \010
- retroceso \b
- HT \011
- tabulador \t
- LF \012
- nueva línea \n
- VT \013
- tabulador vertical \v
- FF \014
- avance de página \f
- CR \015
- retorno de carro \r
- SO \016
- SI \017
- DLE \020
- DC1 \021
- DC2 \022
- DC3 \023
- DC4 \024
- NAK \025
- SYN \026
- ETB \027
- CAN \030
- EM \031
- SUB \032
- ESC \033
- IS4 \034
- FS \034
- IS3 \035
- GS \035
- IS2 \036
- RS \036
- IS1 \037
- US \037
- espacio ' '
- signo de exclamación !
- comillas "
- almohadilla #
- signo del dólar $
- porcentaje %
- et &
- apóstrofo \'
- paréntesis izquierdo (
- paréntesis derecho)
- asterisco *
- signo más +
- coma ,
- guion -
- punto .
- punto .
- barra inclinada /
- barra /
- cero 0
- uno 1
- dos 2
- tres 3
- cuatro 4
- cinco 5
- seis 6
- siete 7
- ocho 8
- nueve 9
- dos puntos :
- punto y coma ;
- menor que <
- igual =
- mayor que >
- interrogación ?
- arroba @
- corchete izquierdo [
- corchete derecho]
- barra inversa \
- barra inversa \\
- circunflejo ^
- acento circunflejo ^
- guion bajo _
- guion bajo _
- acento grave `
- llave izquierda {
- llave izquierda {

- llave derecha }
- llave derecha }
- barra vertical |
- virgulilla ~
- DEL 177
- NULL 0

Tabla de clases de caracteres con nombres (inglés)

La siguiente tabla describe los nombres de las clases de caracteres estándar a los que puede hacer referencia dentro de los paréntesis en las expresiones regulares ([[:class]]). Tenga en cuenta que las clases de caracteres son específicas de ubicación, de modo que las versiones no inglesas de Guardium pueden utilizar un conjunto de nombres de caracteres distinto.

- alnum - Alfanumérico (a-z, A-Z, 0-9)
- alpha - Alfabético (a-z, A-Z)
- blank - Espacio en blanco (espacio en blanco, nueva línea, retorno de carro)
- cntrl - Control
- digit - 0-9
- graph - Gráficos
- lower - Alfabético minúsculas (a-z)
- print - Caracteres imprimibles
- punct - Caracteres de puntuación
- space - Espacio, tabulador, nueva línea y retorno de carro
- upper - Alfabético mayúscula
- xdigit - Dígitos hexadecimales (0-9, a-f)

Ejemplos de expresiones regulares

Puede copiar y pegar cualquiera de las expresiones regulares en un campo que requiera una expresión regular. Al utilizar cualquiera de estos ejemplos, le recomendamos que experimente utilizando la herramienta Crear expresión regular, especificando una variedad de valores coincidentes y no coincidentes, para que comprenda exactamente lo que coincide con la expresión.

Ejemplos de expresiones regulares

Número de la seguridad social (debe tener guiones) [0-9]{3}-[0-9]{2}-[0-9]{4}

Número de teléfono (América del norte: Coincidencias 3334445555, 333.444.5555, 333-444-5555, 333 444 5555, (333) 444 5555 y todas las combinaciones de los mismos) \(?[0-9]{3}\)?[-.]?[0-9]{3}[-.]?[0-9]{4}

Código postal: (Canadá) [ABCEGHJKLMNPRSTVXY][0-9][A-Z] [0-9][A-Z][0-9]

Código postal: (Reino Unido) [A-Z]{1,2}[0-9][A-Z0-9]? [0-9][ABD-HJLNP-UW-Z]{2}

Código postal: (Estados Unidos) (se necesitan 5 dígitos, guion seguido de cuatro dígitos opcionales) [0-9]{5}(?:-[0-9]{4})?

Números de tarjeta de crédito [0-9]{4}[-,]?[0-9]{4}[-,]?[0-9]{4}[-,]?[0-9]{4}

Tema principal: Descubrir

Descubrir y clasificar datos confidenciales en servidores de archivos

La supervisión de la actividad de archivos garantiza la integridad y la protección de los datos confidenciales en servidores de archivos UNIX y Windows.

- Instalación y activación de los componentes de supervisión de actividad de archivos
  Instalar el cliente GIM en el servidor de archivos y utilizarlo para instalar el S-TAP de supervisión de actividad de archivos y el agente de descubrimiento.
- Parámetros GIM de descubrimiento y clasificación de archivos
  Utilice estos parámetros GIM para configurar el descubrimiento y la clasificación de archivos para cada recopilador.
- Personalización de planes de decisiones de FAM
  Los planes de decisiones se utilizan para identificar contenido confidencial en archivos. El agente de descubrimiento de FAM de Guardium proporciona planes de decisiones predeterminados para HIPAA, PCI, SOX y código fuente. Puede cambiar las entidades de clasificación desde los informes resultantes/Panel de control de investigación, utilizando los planes de decisiones predeterminados. También puede crear planes nuevos o modificar planes existentes utilizando IBM Content Classifier Workbench.

Tema principal: Descubrir
Información relacionada:
Supervisión de la actividad de archivos utilizando Guardium (vídeo).

Instalación y activación de los componentes de supervisión de actividad de archivos

Instalar el cliente GIM en el servidor de archivos y utilizarlo para instalar el S-TAP de supervisión de actividad de archivos y el agente de descubrimiento.

Antes de empezar

- Las claves de licencia deben estar instaladas. Consulte Instalar claves de licencia:
- S-TAP debe estar instalado. Es necesario para la supervisión de archivos y la obligatoriedad de políticas.
- El agente de descubrimiento FAM (también conocido como lote FAM o agente FAM) debe ser accesible. Es necesario para el descubrimiento de archivos y la clasificación.

Consejo: Para instalar el agente de descubrimiento FAM satisfactoriamente en AIX, se recomienda establecer el tamaño de datos de proceso en ilimitado modificando las siguientes líneas en /etc/security/limits file: default: data = -1

Acerca de esta tarea

Procedimiento

1. Instale el cliente GIM en el servidor de archivos. Consulte Guardium Installation Manager.
2. Baje los lotes S-TAP y FAM y guárdelos en una unidad accesible. Elija el módulo correcto para su SO de servidor de archivos. El lote de UNIX tiene un nombre como: guard-bundle-FAM_r*****_trunk_*****.gim. El lote de Windows tiene el siguiente aspecto: guard-FAM-guardium_r*****Windows-Server-x86_x64_ia64.gim.
3. En el Gestor central, si lo hay, de lo contrario en un dispositivo, suba e importe el módulo S-TAP y el lote FAM:
   a. Navegue a Gestionar > Instalación de módulo > Subir módulos.
   b. En Subir módulos, pulse Explorar y navegue y seleccione el lote S-TAP. Pulse Subir.
   c. Pulse Explorar y navegue hasta el lote FAM. Pulse Subir.
   d. En Importar módulos subidos, seleccione S-TAP y el lote FAM y pulse Instalar/Actualizar.
4. Instale el S-TAP:
   a. Instale el módulo de S-TAP en el servidor de archivos. Navegue a Gestionar > Instalación de módulo > Configurar por cliente (Antiguo). Para ver todos los clientes registrados, pulse Buscar.
   b. Seleccione su servidor de archivos, o servidores y pulse Siguiente. No hay parámetros S-TAP específicos para la supervisión de actividad de archivo.
   c. Pulse Aplicar a seleccionados y pulse Instalar/Actualizar. Puede instalar ahora o planificarlo para una instalación posterior.
   d. Verifique que el S-TAP se ha instalado correctamente viendo el informe de Guardium, Supervisor de estado de S-TAP (añada el informe desde Mi panel de control). Busque el host de S-TAP para que tenga el sufijo :FAM.
5. Instale y configure el lote FAM:
   a. Navegue a Gestionar > Instalación de módulo > Configurar por cliente (Antiguo). Para ver todos los clientes registrados, pulse Buscar.
   b. Seleccione su servidor de archivos y pulse Siguiente.
   c. Elija el módulo FAM que ha subido. (Para Windows, es posible que necesite desmarcar el recuadro de selección Visualizar solo lotes).
   d. Nota: También puede configurar parámetros de GIM utilizando el mandato grdapi: gim_update_client_params.
      Configure parámetros para el agente de descubrimiento FAM, incluido: SOURCE_DIRECTORIES para los directorios que desee escanear. De forma predeterminada, el agente solo realizará un escaneo básico de la información de titularidad. Para habilitar escaneos basados en planes de decisiones, como para SOX o HIPAA, debe establecer FAM_IS DEEP_ANALYSIS en true. De forma predeterminada, utiliza todos los planes de decisiones predeterminados. Puede especificar qué planes de decisiones desea utilizar. La planificación predeterminada para el escaneo es cada 12 horas y se inicia inmediatamente después de la configuración. Puede cambiarlo utilizando parámetros de GIM FAM_SCHEDULER_HOUR_TIME_INTERVAL, FAM_SCHEDULER_START y FAM_SCHEDULER_REPEAT. Consulte la lista completa de parámetros en Parámetros GIM de descubrimiento y clasificación de archivos.
   e. Pulse Aplicar a seleccionados y pulse Instalar/Actualizar, donde puede instalar de forma inmediata o planificarlo para más tarde.
6. Verifique que el agente de descubrimiento FAM se ha instalado correctamente viendo el informe de Guardium, Supervisor de estado de S-TAP (añada el informe desde Mi panel de control). Busque el sufijo FAM_Agent en la dirección IP del host S-TAP.
7. Para desencadenar el redescubrimiento de archivos más tarde sin desinstalar y volver a instalar el lote FAM:
   a. Elimine los archivos del directorio de trabajo. Si Guardium está instalado en el directorio predeterminado, debe eliminar los archivos de este directorio del servidor de archivos: /usr/local/IBM/modules/FAM/current/files/work
   b. Cambie cualquier parámetro FAM en GIM, por ejemplo, cambiando el intervalo de tiempo de 5 a 10 minutos.
   c. Pulse Aplicar a seleccionados y pulse Instalar/Actualizar.

Resultados

Resultados de Descubrimiento y Clasificación: Cuando la instalación del agente de descubrimiento FAM (rastreador de archivos) ha finalizado, se inicia una ejecución básica para el rastreo de archivos, utilizando la vía de acceso inicial que especificó durante la instalación. Cada vez que el rastreador completa su ejecución, envía un mensaje de estado que se incluye en el informe de Configuración del rastreador de archivos. Este proceso recopila la lista de carpetas y archivos, su propietario, los permisos de acceso, el tamaño y la fecha y hora de la última actualización.

Tema principal: Descubrir y clasificar datos confidenciales en servidores de archivos
Información relacionada:
Funciones de GuardAPI File Activity Monitor
Funciones de GuardAPI File Activity Monitor

Parámetros GIM de descubrimiento y clasificación de archivos

Utilice estos parámetros GIM para configurar el descubrimiento y la clasificación de archivos para cada recopilador.

Configure el descubrimiento y la clasificación de archivos por recopilador. Estos parámetros se pueden configurar durante la instalación o en un momento posterior con GIM (Gestionar > Instalación de módulo > Configurar por cliente) o utilizando el mandato GuardAPI gim_update_client_params. Solo puede actualizar un recopilador a la vez cuando utiliza GuardAPI.

Parámetro GIM	Descripción	Interfaz gráfica de usuario	gr dapi
FAM_CLASSIFICATION_LANGUAGES	Interno. De forma predeterminada, FAM_CLASSIFICATION_LANGUAGES está establecido en inglés. Establézcalo en GenericLanguage para la detección automática de idioma. Para Linux, asegúrese de que su servidor Linux tiene instalado el soporte de idioma necesario. Por ejemplo, para soportar la clasificación de documentos chinos, el soporte de chino debe estar instalado en Linux. Para obtener más información sobre los idiomas soportados por IBM Content Classification, consulte http://www-01.ibm.com/support/knowledgecenter/SSBRAM_8.8.0/com.ibm.classify.workbench.doc/c_WBG_available_languages.htm%23wp9000332?lang=en	X	
FAM_DEBUG	0=Desactivado 1=Activado Los registros del servidor de archivos se recopilan y envían al dispositivo Guardium.	X	
FAM_ENABLED	0 = El agente de descubrimiento de FAM está inhabilitado. 1 = El agente de descubrimiento de FAM está habilitado. Predeterminado 2 = Reiniciar el agente de descubrimiento de FAM. En instalaciones de GIM, está inhabilitado de forma predeterminada, desde la v10.1.4. En instalaciones de S-TAP de shell, el valor predeterminado es habilitado. Para reiniciar FAM: Cambie el parámetro FAM_ENABLED en la interfaz gráfica de usuario de GIM a 2 y aplíquelo a los clientes pulsando Instalar/Actualizar. **Unix:** El servicio FAM en el servidor de archivos debe cambiar el PID mostrándolo como reiniciado (ps -ef | grep fam) y hay una nueva entrada en el informe de interfaz gráfica de usuario predefinido "Configuración del rastreador de archivos". La configuración se revierte a 1 en la interfaz gráfica de usuario de GIM permitiéndole reiniciar de nuevo repitiendo el proceso. **Windows:** El servicio FAM se reinicia, como se muestra en el visor de sucesos (Registros de Windows y sistema `El servicio FAM de IBM Guardium tiene estado detenido` y `El servicio FAM de IBM Guardium tiene estado en ejecución`). No hay **ninguna** entrada nueva en el informe de interfaz gráfica de usuario predefinido "Configuración del rastreador de archivos" y la configuración se mantiene en 2 en la interfaz gráfica de usuario de GIM. Para el siguiente reinicio, cambie el parámetro a 1.	X	
FAM_ICM_CLASS_DECISION_PLANS	Habilita los planes de decisiones incluyendo los nombres de plan y sus entidades de clasificación. DecisionPlanName1{Entity1.1,Entity1.2,..}:DecisionPlanName2{Entity2.1,Entity2.2,..} Establezca una lista delimitada por punto y coma de listas de entidades de planes de decisiones para cada plan de decisiones. Formato: Entidades listadas entre llaves {} y delimitadas por dos puntos. Cuando las llaves están vacías o faltan en algunos planes de decisiones, se presentan todas las entidades de clasificación en los resultados de clasificación del informe de FAM/Panel de control de investigación. Ejemplos de llaves vacías o ausentes: DecisionPlanName1{}:DecisionPlanName2{} DecisionPlanName1:DecisionPlanName2"~		
FAM_ICM_CLASS_THREAD_COUNT	Número de hebras para que utilice el clasificador. El valor predeterminado es 5 y es el valor recomendado.	X	
FAM_ICM_URL	El URL del servidor de IBM Content Classification. El valor predeterminado es http://localhost:18087.	X	
FAM_INSTALLER	Solo Windows. La vía de acceso al paquete del instalador.		

FAM_INSTALL_DIR	Solo Windows. La ubicación en qué se instala el software de Supervisión de actividad de archivos.		
FAM_IS_DEEP_ANALYSIS	False=La clasificación está inhabilitada. Escaneo básico de metadatos y solo permiso de acceso. True=La clasificación está habilitada, en función del contenido del archivo. Si no hay planes de decisiones habilitados (FAM_ICM_CLASS_DECISION_PLANS no está definido), solo se realiza un escaneo básico.	X	
FAM_SCAN_EXCLUDE_DIRECTORIES	Directorios a excluir del descubrimiento y la clasificación. No están soportados los caracteres comodín. Formato: Vía de acceso al directorio completa.	X	
FAM_SCAN_EXCLUDE_REMOTE_DIRECTORIES	True/false. El valor predeterminado es true. Para escanear directorios remotos, establecer en false. Directorios remotos a excluir del descubrimiento y la clasificación. No están soportados los caracteres comodín. En Windows, establecer a algo parecido a: \\\\RemoteMachine\sharefolder\directoryA	X	
FAM_SCAN_EXCLUDE_EXTENSIONS	Excluye las extensiones de archivo especificadas o los documentos sin extensión del escaneo de FAM. Relevante para Windows y Linux. Formato: Lista delimitada por punto y coma. El valor distingue entre mayúsculas y minúsculas. Ejemplos de extensiones excluidas: pdf;txt;doc. Para excluir documentos sin extensión, indique "NO_EXTENSION".	X	
FAM_SCAN_EXCLUDE_FILES	Archivos a excluir del descubrimiento y la clasificación. Formato: Nombre de archivo válido. No están soportados los caracteres comodín.	X	
FAM_SCAN_MAX_DEPTH	Limita la profundidad del escaneo relativa con los directorios de inicio especificados (FAM_SOURCE_DIRECTORIES).	X	
FAM_SCHEDULER_HOUR_TIME_INTERVAL	Frecuencia horaria en que se ejecuta el escaneo de descubrimiento y clasificación. Formato: Entero. El valor predeterminado es 12 horas.	X	
FAM_SCHEDULER_MINUTE_TIME_INTERVAL	Junto con el intervalo de horas, este es el intervalo de tiempo entre escaneos. Por ejemplo, si desea que los escaneos ocurran con 12 horas y 30 minutos de diferencia, especifique 12 para las horas y 30 para los minutos. Formato: Entero.	X	
FAM_SCHEDULER_REPEAT	True = Repetir el proceso de descubrimiento en el intervalo de tiempo especificado. False = No repetir el escaneo.	X	
FAM_SCHEDULER_START_TIME	Tiempo de la activación inicial de los procesos de descubrimiento y clasificación. Formato: MM-DD-AAAA HH:mm Por ejemplo, si especifica 01-02-2016 18:00, el escaneo se iniciará a las 18 h del 2 de enero de 2016. Si el intervalo de tiempo es de 12 horas, el proceso se ejecutará cada día a las 18 h y a las 6 h.	X	
FAM_SERVER_PORT	El puerto del recopilador de Guardium, 16022.	X	
FAM_SOURCE_DIRECTORIES	El directorio o directorios desde los que se inicia el escaneo. No están soportados los caracteres comodín. Ejemplo: /home/test. Formato: Lista de conjuntos de directorios de origen de FAM delimitados por punto y coma. Ejemplo: %IBM_FAM_HOME%/test/dir1;%IBM_FAM_HOME%/test/dir2 ~ Utilice FILE_SYSTEM_ROOTS para escanear todos los archivos en el servidor. No se recomienda especialmente si el servidor tiene muchos archivos.	X	

Tema principal: Descubrir y clasificar datos confidenciales en servidores de archivos
Información relacionada:
GIM: Interfaz gráfica de usuario
GIM: CLI

Personalización de planes de decisiones de FAM

Los planes de decisiones se utilizan para identificar contenido confidencial en archivos. El agente de descubrimiento de FAM de Guardium proporciona planes de decisiones predeterminados para HIPAA, PCI, SOX y código fuente. Puede cambiar las entidades de clasificación desde los informes resultantes/Panel de control de investigación, utilizando los planes de decisiones predeterminados. También puede crear planes nuevos o modificar planes existentes utilizando IBM Content Classifier Workbench.

Antes de empezar

Instale IBM Content Classification 8.8 en una estación de trabajo de Windows que se pueda conectar a su entorno de Guardium.

Durante la Supervisión de actividad de archivos, el usuario de instalación de GIM debe configurar el Plan de decisiones de ICM configurándolo en la página de configuración de GIM de Supervisión de actividad de archivos.

El usuario debe configurar la lista de planes de decisiones (categorías) con entidades (campos NVP) para cada plan de decisiones delimitado por dos puntos.

La Supervisión de actividad de archivos utiliza esta configuración para clasificar contenido.

El cliente debe ser capaz de configurar todas las entidades posibles para cada plantilla de planes de decisiones, disponibles durante la instalación de la Supervisión de actividad de archivos.

La clasificación de planes de decisiones solo aparecerá cuando el archivo sea confidencial y la clasificación no esté vacía.

Después de la instalación de la Supervisión de actividad de archivos, hay disponibles cuatro plantillas de plan de decisiones:

- HIPAA, PCI, SOX, Fuente
- El plan de decisiones HIPAA se utiliza para encontrar información médica.
- PCI para encontrar números de tarjeta de crédito.
- SOX para documentos financieros.

El plan de decisiones "Fuente" hace referencia a dos bases de conocimientos (CodeKB y DocumentTypeKB) que están cargadas por defecto una vez que se configura el plan de decisiones Fuente.

Aquí está la lista de entidades posibles para cada plan de decisiones proporcionado listo para usar con la Supervisión de actividad de archivos y se puede configurar mediante GIM.

HIPAA

SSN, Name, License, GovermentID, PassportContext, BankAccount, Address, IPAddress, EmailAddress, URL, Phone, CreditCard, possibleHealthPlan, Confidential_match, HIPAA_match

PCI

SSN, Name, License, GovermentID, PassportContext, BankAccount, Address, IPAddress, EmailAddress, URL, Phone, BankAccountContext, CreditCard, CreditContext, containCardIssuer, PCI_match, Confidential

SOX

SSN, Name, License, GovermentID, PassportContext, BankAccount, Address, IPAddress, EmailAddress, URL, Phone, BankAccountContext, CreditCard, CreditContext, containCardIssuer, piiMatch, Confidential, SOXContext, SOX_match

Source

containDate,hasSSN, hasBirthDate, containCardIssuer, hasCreditCard, PCIViolation, HIPAA_Match, ConfidentialMatch, Source_match

Un plan de decisiones es una recopilación de reglas que puede configurar para determinar como IBM Classification Module clasifica los elementos de contenido. Las reglas consisten en desencadenantes y acciones. Un desencadenante determina las condiciones que se deben cumplir para iniciar una acción. Una acción determina como se debe clasificar el documento. Un plan de decisiones también puede hacer referencia a una o más bases de conocimiento para combinar la clasificación de regla basada en palabras clave con una clasificación estadística basada en texto.

Una base de conocimiento es un conjunto de datos recopilados que se utilizan para analizar y categorizar elementos de contenido. La base de conocimiento refleja los tipos de datos que espera que gestione el sistema. Antes de que la base de conocimientos pueda analizar texto, se debe entrenar con un número suficiente de elementos de contenido de ejemplo clasificados correctamente en categorías. Una base de conocimiento entrenada puede calcular una medida numérica de relevancia de un elemento para cada categoría.

Nota: ICM no es capaz de trabajar con planes de decisiones con nombres chinos. Se soportan los documentos de contenido y las reglas de plan de decisiones en chino pero no los nombres de planes en chino.
Nota: No está soportada la distribución de planes de decisión desde el Gestor central a las unidades gestionadas.
Nota: Los resultados de clasificación para cada plan de decisiones se deben especificar mediante entidades debidamente reconocidas y configuradas. La clasificación solo aparecerá cuando el archivo sea confidencial y la clasificación no esté vacía. En el nivel de depuración, existe documentación relativa a los errores de ICM y los fallos de los planes de decisiones.

Acerca de esta tarea

Para el propósito de esta descripción, supongamos que su empresa tiene un proyecto confidencial llamado "ProjectA". Desea identificar y supervisar todos los archivos que contienen esta serie.

Procedimiento

1. Utilice el menú Inicio de Windows para abrir el entorno de trabajo de clasificación de IBM Content Classification 8.8.
2. En el diálogo Abrir proyecto, pulse Nuevo....
3. En el diálogo Proyecto nuevo, elija Plan de decisiones para el tipo de proyecto. Especifique un nombre para este plan de decisiones, como `ProjectA_DP`. Especifique una descripción si desea una.
4. En el diálogo Opciones de proyecto nuevo, seleccione Crear un proyecto vacío.
5. En el Explorador de proyectos, pulse Archivos de lista de series y palabras. En el diálogo Archivos de lista de series y palabras, pulse Nuevo... para crear un nuevo archivo. En el diálogo Nuevo archivo, elija Lista de palabras para el tipo de archivo y elija un nombre para el archivo. En este ejemplo lo llamaremos `Names`. Wordlist_Names.txt aparece en la lista de archivos.
6. Efectúe una doble pulsación en el nombre del archivo para editar el archivo. Inserte una sola línea con la serie `~ProjectA~` y guarde el archivo.
7. En el Explorador de proyectos, pulse Plan de decisiones > Nuevo grupo > Nueva regla. Cambie el nombre de la regla a `ProjectA`.
8. En el diálogo Nueva regla, abra el separador Desencadenante. Pulse Condición.
9. Elija Desencadenar cuando los campos contienen palabras o expresiones específicas. Elija Archivo de lista de palabras. Pulse Aceptar.
10. Abra el separador Acción. Pulse Añadir nueva regla.
11. Seleccione Acciones avanzadas de la lista de Tipo de acción. Elija la acción Establecer el campo de contenido. Este campo de contenido se crea cuando se activa el desencadenante específico. El campo de contenido se puede visualizar en los informes de FAM.
12. En el diálogo Añadir acción, especifique `ProjectA_match` como el nombre del campo de contenido y especifique `found` en el campo de valor.
13. Importe el conjunto de contenido en el proyecto del plan de decisiones.

a. Cree un documento de texto que contenga la serie "ProjectA".
b. En el Explorador de proyectos, expanda el proyecto ProjectA_DP. Pulse con el botón derecho en Conjunto de contenido y elija Importar conjunto de contenido.
c. Pulse Archivos de una carpeta del sistema de archivos. Navegue al archivo que ha creado en el paso a. Pulse Siguiente, a continuación, pulse Siguiente, luego Siguiente y luego Finalizar.

14. Verifique que su definición es satisfactoria.
    a. En el Explorador de proyectos, abra el separador Conjunto de contenido. Pulse con el botón derecho en su archivo y elija Ejecutar elemento a través del plan de decisiones.
    b. En el diálogo Elemento analizado, expanda el plan de decisiones y el grupo. Verifique que Regla:ProjectA está marcado [Desencadenado].
    c. Pulse Campos de contenido.... En el diálogo Seleccionar campos de contenido, verifique que se muestra "ProjectA_match" en el recuadro de Campos cambiados y "found" en el recuadro de contenido.
15. En el Explorador de proyectos, pulse Proyecto > Guardar para guardar el proyecto ProjectA_DP.
16. En el Explorador de proyectos, pulse Proyecto > Exportar para exportar el proyecto ProjectA_DP a un archivo dpn.
17. Utilice GIM para enviar el archivo dpn a los servidores de archivos donde desee utilizar el plan de decisiones.

Tema principal: Descubrir y clasificar datos confidenciales en servidores de archivos

Optimización de titularidades

La Optimización de titularidades media entre el rol del administrador de base de datos, para proporcionar a los usuarios las titularidades necesarias para realizar sus trabajos de forma eficiente y, el rol de seguridad para mantener las titularidades tan precisas y mínimas como sea posible para evitar vulnerabilidades del sistema.

La optimización de la titularidad se ha incorporado en Guardium V10.1.2.

Las situaciones aparecen de forma natural durante la gestión diaria del sistema y provoca vulnerabilidades, por ejemplo:

- Acceso generalizado
- Un privilegio que se dio a un usuario para un uso puntual pero que no se ha eliminado después.
- Cambios de usuarios y tablas a lo largo del tiempo, que dan como resultado usuarios y tablas inactivas.
- Privilegios que se pasan de un usuario a otro.

Las titularidades requieren vigilancia constante. Por ejemplo, las Amenazas Persistentes Avanzadas (APT) se originan normalmente con una de estas entradas traseras del sistema.

La optimización de titularidades analiza constantemente los privilegios y las acciones de usuario y proporciona recomendaciones que señalan acciones específicas que tienen como objetivo minimizar el acceso del usuario a solo lo necesario. El análisis lo realiza completamente el sistema. El administrador revisa los resultados, examina cada caso y realiza las acciones adecuadas, por ejemplo, suprimir privilegios a un usuario de BD o eliminar roles inactivos.

También puede investigar los cambios de titularidades de la semana pasada, una lista completa de usuarios y roles, los privilegios de orígenes de datos junto con su uso real y las justificaciones simuladas de una combinación usuario-rol específica. Estas vistas proporcionan información relevante para las recomendaciones y también son puntos de partida para otras investigaciones.

Las ventajas de la optimización de titularidades sobre los informes de Guardium es que consolidan información de todos los tipos de bases de datos (que aparece en varios informes de Guardium) y añade nuevos análisis a sus informes completos y consolidados, simplificando la gestión de titularidades y, por tanto, aumentando la seguridad del sistema.

La optimización de titularidades soporta los tipos de base de datos: Microsoft SQL Server y Oracle. No soporta bases de datos contenidas de SQL. (Los informes de Guardium son por tipo de base de datos).

La supervisión de la actividad de la optimización de titularidades está limitada a los datos actualmente supervisados por Guardium. La precisión de las recomendaciones, el explorador de titularidades y los análisis de probabilidades dependen de la importancia de los datos supervisados. Para maximizar por completo el potencial de esta herramienta, configure los parámetros userScope y objectScope y considere la posibilidad de modificar la política de seguridad.

Los usuarios que están inactivos desde el momento en que inicia la supervisión con la optimización de titularidades no se incluyen en los informes de optimización de titularidad. Para observar a un usuario específico supervisado pero que no tiene ninguna recomendación, compruebe manualmente la actividad del usuario ya sea a través del explorador de titularidades o en cualquiera de las otras herramientas de supervisión de actividad de Guardium. Si la política se ha definido correctamente las herramientas tienen toda la información.

El análisis de titularidades se realiza por recopilador y solo opera en los orígenes de datos que configura por grdapi.

La característica debe recopilar soporta la optimización de titularidades. Consulte Información básica para el soporte de IBM.

Acceda a la optimización de titularidades desde Descubrir > Titularidades de base de datos > Optimización de titularidades

- Habilitar y configurar la optimización de titularidades
  Uso de los mandatos grdapi para habilitar y configurar la optimización de titularidades.
- Novedades de la optimización de titularidades
  El separador Novedades resume las adiciones y cambios realizados en el sistema durante la semana del calendario, de domingo a domingo.
- Usuarios y roles de optimización de titularidades
  El separador Usuarios y roles lista todos los usuarios y sus roles para todos los orígenes de datos habilitados para la optimización de titularidades en este recopilador.
- Recomendaciones de optimización de titularidades
  Las recomendaciones señalan acciones específicas que tienen como objetivo minimizar el acceso del usuario a solo lo que es necesario.
- Examinar las titularidades de la optimización de titularidades
  Utilice las vistas y filtros de esta ventana para ver el nivel de actividad de las titularidades y el linaje de las titularidades.
- Probabilidad de optimización de titularidades
  La probabilidad muestra la posible justificación para la titularidad de un usuario específico con uno o más verbos determinados en un objeto concreto (independientemente de si la titularidad existe o no).

Tema principal: Descubrir

Habilitar y configurar la optimización de titularidades

Uso de los mandatos grdapi para habilitar y configurar la optimización de titularidades.

Todos los mandatos se ejecutan en el Recopilador y utilizan los orígenes de datos ya definidos de Guardium. Primero debe habilitar la característica en el Recopilador, a continuación, especifique los orígenes de datos y habilite las características específicas.

Los resultados más precisos se obtienen ajustando los datos incluidos en la optimización de titularidades.

Las características Usuarios y roles y Examinar titularidades están habilitadas de forma predeterminada, sin embargo, debe establecer extractActivity y extractEntitlement en `true` para extraer los datos relevantes. Las otras tres características (Novedades, Recomendaciones y Probabilidad) se habilitan de forma individual. Por ejemplo, puede habilitar Recomendaciones mientras deja Probabilidad inhabilitada.

Las recomendaciones de titularidades utilizan un subconjunto de datos, filtrados por los parámetros userScope y objectScope. Examinar titularidades utiliza el parámetro userScope para filtrar los datos. Ambos parámetros especifican uno o más grupos de Guardium. Lo más probable es que cree grupos específicos para utilizarlos con esta finalidad. Defina los grupos para extraer solo los datos que desea, para minimizar el almacenamiento y el procesamiento. Los grupos deben tener Auditoría completa para que se analicen todos los datos y los resultados sean concluyentes. Cuando utiliza grupos con Auditoría completa, Examinar titularidades muestra todos los derechos de todos los usuarios, independientemente de su actividad. Los usuarios que están fuera de la definición de userScope aparecen en la ventana pero su recuento de actividad es "Desconocido".

El método recomendado es evaluar cuidadosamente y diseñar su esquema de recopilación de datos de forma que no tenga que cambiarlo. Esto es así por dos motivos: Cada vez que cambia la configuración, se tarda una semana en generar los datos para los informes. Los datos se comparan con los de las 3 semanas anteriores y cuando cambia la definición de los datos, la comparación es menos significativa las tres primeras semanas.

Los datos están presentes en cada separador desde el primer domingo tras habilitar la característica individual.

Consulte todos los detalles de mandatos en Funciones de optimización de titularidades de GuardAPI.

Requisitos previos

- La búsqueda rápida debe estar habilitada. (Es necesaria para Probabilidad, Recomendaciones y actualización de actividad en el explorador de titularidades).
- El usuario que configura la optimización de titularidades debe tener permisos para todas las tablas de metadatos y de esquema en los orígenes de datos configurados.

Habilitar entitlement_optimization en el Recopilador

Habilita la optimización de titularidades en el Recopilador.

Sintaxis:

grdapi enable_entitlement_optimization

Inhabilitar entitlement_optimization en el Recopilador

Inhabilita la optimización de titularidades en el Recopilador.

Sintaxis:

grdapi disble_entitlement_optimization

Añadir origen de datos a la optimización de titularidades

Añade uno o más orígenes de datos a la optimización de titularidades y habilita el análisis individual.

Sintaxis:

grdapi add_datasource_to_entitlement_optimization datasourceName=[datasource] isEnabled=[true/false] userScope=[USER SCOPE] objectScope=[OBJECT SCOPE] extractActivity=[true/false] extractEntitlement=[true/false] generateRoleClusters=[true/false] generateNews=[true/false] generateRecommendations=[true/false]

Utilice esta tabla para determinar las extracciones que necesita, por característica:

Tabla 1. Parámetros enable_entitlement_optimization necesarios por tipo de análisis

	Novedades (generateNews)	**Usuarios y roles**	**Recomendaciones (generateRecommendations)**	**Examinar titularidades**	**Probabilidad (generateRoleClusters)**
extractActivity				X	X
extractEntitlement	X	X	X	X	

Eliminar orígenes de datos de la optimización de titularidades

Elimina uno o más orígenes de datos desde la optimización de titularidades de modo que no se recopilan datos.

remove_datasource_from_entitlement_optimization datasourceName=[nombre de origen de datos]

Modificar parámetros de origen de datos de titularidades

Modifica los parámetros para un origen de datos que ya está habilitado para la optimización de titularidades.

Sintaxis:

grgapi set_entitlement_datasource_parameter datasourceName=[nombre de origen de datos] parameterName=[valor] parameterName=[valor]

Donde el parámetro parameterName es:

isEnabled

userScope

objectScope

extractActivity

extractEntitlement

generateRoleClusters

generateNews

generateRecommendations

filterTempObjects

filterIgnoreVerbs

Ver la información de optimización

Sintaxis:

grdapi get_entitlement_optimization_info

Salida típica:

```
Entitlement Optimization is enabled
===================================
Datasource: SCALE-DB16
===================================
isEnabled: true
userScope:
objectScope:
extractActivity: true
extractEntitlement: true
generateRoleClusters: true
generateNews: true
generateRecommendations: true
filterTempObjects: true
filterIgnoreVerbs: true
```

Tema principal: Optimización de titularidades

Novedades de la optimización de titularidades

El separador Novedades resume las adiciones y cambios realizados en el sistema durante la semana del calendario, de domingo a domingo.

Los datos se presentan en el separador desde el primer domingo después de crear la característica.

El separador Novedades presenta:

- El número de usuarios, roles y objetos nuevos y el número de bases de datos asociadas con estas adiciones.
- El número de receptores y otorgantes de autorización y el número de otorgamientos.

Área de búsqueda

Busque tendencias, por ejemplo, profundizando para encontrar:

- Tipos o cantidades de cambios inusuales en las titularidades.
- Los receptores y otorgantes de autorización más activos.

Pulse Detalles en cualquier tema para abrir una tabla detallada de las adiciones. Por ejemplo, los detalles de los nuevos usuarios son el nombre de servidor y de servicio.

Tema principal: Optimización de titularidades

Usuarios y roles de optimización de titularidades

El separador Usuarios y roles lista todos los usuarios y sus roles para todos los orígenes de datos habilitados para la optimización de titularidades en este recopilador.

Los datos se presentan en el separador desde el primer domingo después de crear la característica.

Este separador está basado en el informe de usuarios y roles estándar de Guardium que presenta los datos en un solo tipo de base de datos. Presenta:

- Host
- Nombre de servicio
- Tipo de BD
- Receptor de autorización
- Tipo de receptor de autorización
- Rol

Puede utilizar las funciones estándar del Creador de informes, a las que se accede mediante los iconos situados sobre la tabla.

Tema principal: Optimización de titularidades

Recomendaciones de optimización de titularidades

Las recomendaciones señalan acciones específicas que tienen como objetivo minimizar el acceso del usuario a solo lo que es necesario.

Los datos se presentan en el separador desde el primer domingo después de crear la característica.

El sistema está continuamente evaluando usuarios y privilegios. El informe de recomendaciones de titularidades semanal está basado en los datos de las últimas 3 semanas (de forma predeterminada), de modo que cada nuevo informe se solapa con los datos del informe anterior. El separador Recomendaciones es equivalente al informe Recomendaciones en "Informes", que se puede habilitar como informe distribuido.

Si ha personalizado el parámetro userScope, las recomendaciones solo incluirán los usuarios de los grupos de usuarios especificados. Los parámetros userScope y objectScope se utilizan para definir de forma explícita el ámbito de las recomendaciones. Para poder maximizar la precisión de las recomendaciones en relación con usuarios y objetos, los usuarios y objetos en los grupos especificados deben tener auditoría completa.

Todas las recomendaciones deben ser completamente investigadas por el administrador, profundizando en un servidor, base de datos, objeto y tipo de recomendación específicos, antes de la implementación.

La parte superior del separador contiene un gráfico circular que muestra las recomendaciones por tipo. La tabla de la parte inferior de la ventana lista las recomendaciones. Puede modificar el informe de recomendaciones utilizando los iconos de informe estándar, exportar el informe pulsando Exportar y correlacionarlo con una API pulsando Acciones.

Los tipos de recomendación son:

Tabla 1. Tipos de recomendación

Tipo	Serie	Detalles
ANOMAL USER	El usuario {object} tiene actividad anómala dentro del rol {source}.	El recuento de actividad de usuario dentro de un rol específico es anómalo. Esto significa que el usuario es mucho más activo o mucho menos activo que los otros usuarios.
ALERT ACTIVITY (Usuario ad-hoc)	El usuario {source} ha utilizado el {verb}-{object} de privilegio pero no se ha encontrado ninguna titularidad.	Un usuario ad hoc típico se otorga a sí mismo permisos, realiza una acción y, luego, elimina el permiso. Los usuarios pueden identificarse de forma errónea como ad hoc debido a las diferencias de tiempo entre los cambios de titularidad y sus actividades. Utilice las herramientas de Supervisor de actividad de Guardium para determinar si el privilegio es justificado o no.
DORMANT_USER	Eliminar el usuario {object} inactivo o vacío.	El usuario no tiene un privilegio asignado o no tiene actividad en el intervalo indicado.
DORMANT_ROLE	Eliminar el rol {role} inactivo o vacío.	No hay usuarios, no hay actividad por cualquier usuario o privilegios vacíos.
REVOKE_FROM_USER	Revocar {verb}-{object} del usuario {source}.	El usuario no ha realizado ninguna actividad en el objeto relevante o verbo.
REVOKE_FROM_ROLE	Revocar {verb}-{object} del rol {source}	TODOS los usuarios en el rol específico no han realizado ninguna actividad en el objeto o verbo.
REMOVE_FROM_ROLE	Eliminar usuario {object} del rol {source}	El usuario no ha utilizado ninguno de los privilegios que le han otorgado por el rol.
INACTIVE DATABASE	La base de datos no tiene actividad.	Si la base de datos no utilizada no se puede justificar, elimínela.

Tema principal: Optimización de titularidades

Examinar las titularidades de la optimización de titularidades

Utilice las vistas y filtros de esta ventana para ver el nivel de actividad de las titularidades y el linaje de las titularidades.

Los datos se presentan en el separador desde el primer domingo después de crear la característica. Después del primer domingo, las actividades se actualizan diariamente.

Esta información es útil para la investigación de titularidades general y para evaluar más las recomendaciones del informe de recomendaciones. La vista predeterminada en esta ventana es un gráfico de barras de los orígenes de datos con mayor tasa de privilegios no utilizados.

El explorador de titularidades muestra todas las titularidades de los orígenes de datos definidos en grdAPI que tienen disponible extractEntitlement. Esto es cierto si la recopilación de actividad está desactivada y si los ámbitos de usuario y objeto están definidos. Puede buscar y ver los permisos de todos los usuarios en cualquier momento.

Los resultados del campo de recuento de actividad se ven afectados por el parámetro userScope, de la manera siguiente:

- Los usuarios que están incluidos en userScope:
-
    - Los usuarios activos aparecen en verde y tienen resultados numéricos en la columna de recuento de actividad.
    - Los usuarios no activos aparecen en rojo y el recuento de actividad es "No está activo".
- Los usuarios que no están incluidos en userScope:
    - Los usuarios activos aparecen en verde y tienen resultados numéricos en el recuento de actividad.
    - Los usuarios no activos aparecen en gris y el recuento de actividad es "Desconocido".

Las investigaciones típicas son:

- Determinar para qué objetos tiene permisos el usuario y si los utiliza.
- Determinar si un usuario ha utilizado sus permisos en un objeto en el momento específico en que tenía permiso.
- ¿Hay permisos que se hayan utilizado más de lo previsto?

- ¿Hay permisos que solo se hayan utilizado una vez?
- ¿Cuál es el linaje de los permisos que se han utilizado inusualmente: Explícito o implícito, heredado de un rol padre o de una jerarquía de rol?

Para obtener más detalles sobre cómo se utiliza un privilegio específico, con SQL completo, puede buscar actividad de datos (Investigar > Buscar actividad de datos), pulse el botón derecho sobre el usuario de BD o el programa fuente en la tabla de resultados y seleccione SQL completo por usuario de BD.

Las titularidades no utilizadas son normalmente:

- Acción raramente realizada pero titularidad válida, por ejemplo, la generación un informe trimestral.
- No utilizadas y, por lo tanto, no justificadas (punto de vulnerabilidad).

Para ver el uso de las titularidades en un servicio específico en un servidor específico:

1. En el lado izquierdo, seleccione una IP de servidor y un servicio.
2. Filtre por uno o más: Nombre, Nombre de objeto.
3. Opcionalmente, especifique un Verbo o un rango de fecha.

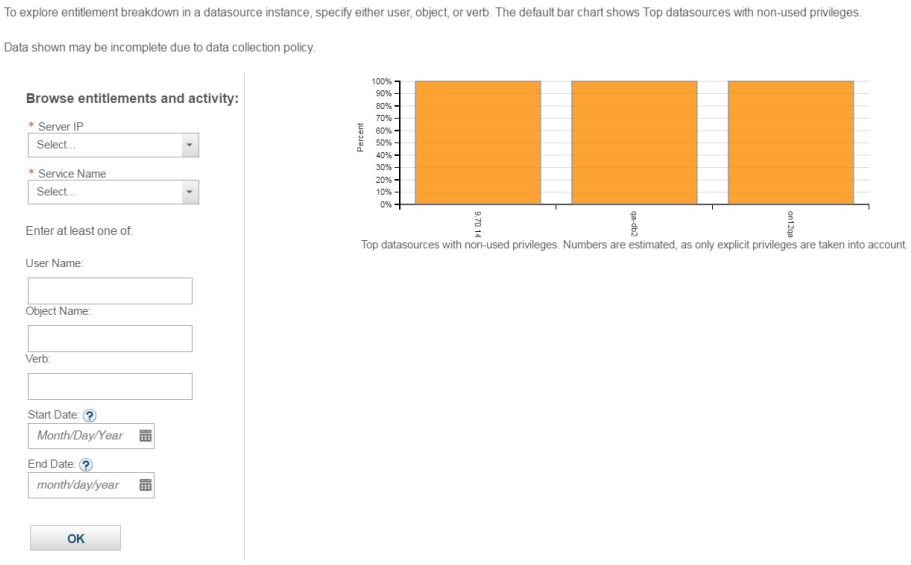


Figura 1. Selección de criterios de titularidad

La tabla presenta el tipo de receptor de autorización, el receptor de autorización, el verbo, el nombre, el recuento de actividad y el linaje. Un usuario puede tener varios linajes de privilegios: Explícito o implícito, heredado de un rol padre o de una jerarquía de rol.

Tema principal: Optimización de titularidades

Probabilidad de optimización de titularidades

La probabilidad muestra la posible justificación para la titularidad de un usuario específico con uno o más verbos determinados en un objeto concreto (independientemente de si la titularidad existe o no).

Los datos están disponibles en este separador desde el primer domingo después de crear la característica.

Guardium analiza el comportamiento de usuarios similares para producir la posible justificación, que, en algunos casos, proporciona información altamente relevante. El análisis puede ser útil cuando examina titularidades no utilizadas y la recomendación REVOKE_FROM_USER. Es una indicación general y se debe utilizar junto con otras características de optimización de titularidades.

Especifique estos detalles y pulse Aceptar para generar la probabilidad:

- Nombre de usuario
- Nombre de objeto
- Verbo (uno o más)
- IP de servidor
- Nombre de servicio

Las respuestas posibles son:

- La probabilidad de que este usuario de BD utilice este privilegio es **n%**. Una probabilidad del 100% indica que el usuario ha utilizado la actividad por lo menos una vez.
- No se ha podido encontrar el origen de datos en el servidor.
- El objeto y el usuario de BD no se encuentran en el ámbito.
- No se han encontrado pruebas suficientes para el usuario de BD y el privilegio: O el usuario/objeto/verbo no existe en la base de datos seleccionada o no se ha encontrado actividad para el usuario o no se ha encontrado actividad para el objeto o tupla de verbo. Arreglos posibles: Espere a que se ejecute la recopilación de actividad; asegúrese de que la entrada se ha especificado correctamente.

Tema principal: Optimización de titularidades

Protección

Después de identificar las bases de datos y los sistemas de archivos que contienen datos confidenciales, puede llevar a cabo varios pasos para proteger esos datos. Las opciones de protección incluyen el enmascaramiento de datos, creación de alertas personales en base al acceso a los datos y el establecimiento de políticas que obliguen

el cumplimiento de restricciones de acceso.

- Líneas base
  Una línea base es un perfil de mandatos de acceso ejecutados en el pasado, que ayuda a identificar la actividad normal y el comportamiento anómalo (incoherente con o desviándose de un comportamiento que es habitual, normal o esperado).
- Políticas
  Una política de seguridad contiene un conjunto ordenado de reglas que se deben aplicar al tráfico observado entre servidores y clientes de base de datos. Cada regla se puede aplicar a una solicitud desde un cliente o a una respuesta desde un servidor. Se pueden definir varias políticas y se pueden instalar varias políticas en un dispositivo Guardium al mismo tiempo.
- Alertas de correlación
  Una alerta es un mensaje que indica que se ha detectado una excepción o una infracción de una regla de política.
- Señalización de sucesos a través de las alertas de correlación
  Desencadenar una alerta de correlación si hay más de quince errores de SQL en las últimas tres horas para un usuario individual cualquiera de la aplicación.
- Gestión de incidencias
  La aplicación IIM (Integrated Incident Management) proporciona una interfaz de usuario empresarial con automatización del flujo de trabajo para el seguimiento y resolución de incidencias de seguridad de base de datos.
- Gestión de la revisión de las incidencias de seguridad de varias bases de datos
  Gestión de incidencias - Seguimiento y resolución de incidencias de seguridad de base de datos.
- Reescritura de consultas
  La funcionalidad de reescritura de consultas proporciona un control de acceso preciso para las bases de datos mediante la interceptación de consultas de bases de datos y su reescritura en función de los criterios definidos en las políticas de seguridad.
- Reglas y políticas de la actividad de archivos
  La supervisión de la actividad de archivos garantiza la integridad y la protección de los datos confidenciales en servidores de archivos UNIX y Windows.

Líneas base

Una línea base es un perfil de mandatos de acceso ejecutados en el pasado, que ayuda a identificar la actividad normal y el comportamiento anómalo (incoherente con o desviándose de un comportamiento que es habitual, normal o esperado).

El Creador de línea base genera una línea base examinando la actividad registrada con anterioridad y con la disponible actualmente en el sistema Guardium.

Cuando se incluye en una política de seguridad, la línea base se convierte en una regla de línea base, permitiendo todo el acceso a la base de datos que se haya incluido en la línea base.

Una regla de línea base en una política tiene las características siguientes:

- Sólo puede haber una regla de línea base.
- La acción de regla de línea base es siempre Permitir, lo que significa aceptar el mandato y no continuar con la regla siguiente de la política.
- Cuando la regla de línea base se añade a la política, se coloca en primer lugar en la lista de reglas. Se puede mover a cualquier lugar del conjunto de reglas (que se evalúan en secuencia), según sea apropiado para la política.
- Una vez que una regla de línea base se ha incluido en una política, no se puede quitar.

Atención: El Creador de línea base y su funcionalidad está en desuso desde Guardium V10.1.4.

El Creador de políticas puede generar reglas de política sugeridas a partir de la línea base. Las reglas sugeridas se pueden editar e incluir en la política delante de la regla de línea base, de modo que se puedan tomar acciones alternativas (alertas, por ejemplo) para algunos mandatos vistos en el periodo de línea base. Además, un examen de las reglas sugeridas proporciona información valiosa sobre los patrones de tráfico reales observados (tipos de mandatos y frecuencia).

El Creador de línea base proporciona la posibilidad de controlar lo que se incluye en la línea base, de varias formas:

- Especificando un umbral para controlar cuántas apariciones de un mandato se deben ver antes de que el mandato se incluya en la regla. Un umbral de uno incluye todos los mandatos observados, mientras que un umbral de 1.000 sólo incluye los mandatos que se dan 1.000 veces o más.
- Controlando la sensibilidad de uno o más atributos. Por ejemplo, si la línea base es sensible al usuario de base de datos, sólo incluirá mandatos para usuarios específicos. Los usuarios que no ejecutaron el mandato durante el periodo de línea base podrían no estar autorizados por la regla de línea base.
- Mediante la limitación de las conexiones incluidas para subconjuntos de direcciones IP de cliente y servidor. La línea base siempre especifica una única máscara de red de cliente y una única máscara de red de servidor. Cada máscara puede ser tan inclusiva o tan exclusiva como sea necesario.
- Fusionando datos de diferentes periodos de tiempo. Es posible que haya tráfico que se produzca durante periodos de tiempo no contiguos que deban incluirse en la línea base. Puede fusionar los datos de cualquier número de periodos de tiempo en una única línea base. Además, los datos se pueden filtrar para direcciones de servidor y cliente específicas.

Acerca de la sensibilidad de la línea base

La sensibilidad de la línea base se puede basar en cualquier combinación de lo siguiente (cada aspecto se describe más detalladamente a continuación):

- Usuario de base de datos
- Protocolo de base de datos
- Versión del protocolo de base de datos
- Periodo de tiempo
- Programa fuente
- Secuencia

La sensibilidad de la línea base depende de un umbral especificado, que define el número mínimo de veces que un mandato debe observarse durante el periodo de línea base para incluir ese mandato en la línea base.

Si no se selecciona ninguna sensibilidad, cada mandato que exceda el umbral se incluirá en la línea base.

Si se selecciona un único tipo de sensibilidad, se mantendrá un recuento independiente de cada mandato para cada valor del tipo de sensibilidad (usuario de base de datos, por ejemplo).

Si se seleccionan varios tipos de sensibilidad, se mantienen recuentos distintos de cada mandato para cada combinación de valores para cada tipo seleccionado (por ejemplo, para cada combinación de usuario de base de datos y programa fuente). Por lo tanto, con cada tipo de sensibilidad incluido, el número de combinaciones puede aumentar drásticamente.

Acerca de la sensibilidad de secuencia

Si la línea base es sensible a la secuencia de mandatos, entonces cuando se incluya en una política, la regla de línea base solo permitirá las secuencias de mandatos observadas durante el periodo de línea base. Para ilustrarlo con un ejemplo muy sencillo: si las dos únicas secuencias de mandatos observadas en el periodo de línea base son A-B y B-C, la tabla siguiente ilustra qué secuencias de mandatos estarán permitidas por dicha regla de línea base.

Tabla 1. Acerca de la sensibilidad de secuencia

Secuencia de mandatos	Permitida
A - B	S
A - todo lo demás	N
B - C	S
B - todos lo demás	N
Cualquiera excepto A	N

Acerca de la sensibilidad del periodo de tiempo

Cuando la línea base es sensible al periodo de tiempo, se mantienen recuentos independientes para cada periodo de tiempo definido. Si se definen periodos de tiempo solapados (lo que es una situación normal), un mandato se contabilizará sólo una vez, en el periodo de tiempo más restrictivo durante el cual se ejecuta. Si el periodo de tiempo no es contiguo, por ejemplo, de 00:00 a 08:00 cada día de la semana - sólo se tiene en cuenta un segmento contiguo del periodo de tiempo (ocho horas en el ejemplo).

Para ilustrar cómo el Creador de líneas base asigna solicitudes a periodos de tiempo, suponga que el sábado se incluye en tres periodos de tiempo:

- 24x7 (24 horas, 7 días a la semana)
- Sábado (sólo 24 horas)
- Fin de semana (48 horas - sábado y domingo)

Puesto que el periodo de tiempo Sábado es el más restrictivo (sólo 24 horas), todas las solicitudes con indicación de fecha y hora del sábado se contarán en dicho periodo de tiempo, y no en los periodos de tiempo más inclusivos de 7x24 o Fin de semana.

Acerca de las líneas base en entornos del Gestor central y de agregación

Si hay varios dispositivos de Guardium en un entorno de agregación y/o de gestor central, existe un punto importante que debe tenerse en cuenta al generar y utilizar líneas base:

Las líneas base se generan utilizando sólo los datos disponibles actualmente en el dispositivo que está generando la línea base.

Esto significa que:

- Una línea base generada en un recopilador se creará utilizando únicamente el tráfico disponible en dicha unidad.
- Una línea base creada en un agregador se creará a partir de los datos disponibles actualmente en el agregador, que normalmente se habrán enviado desde varios recopiladores durante un periodo de tiempo.
- Una línea base generada en un Gestor central que no sea un agregador estará vacía, ya que un Gestor central no recopila datos (a menos que también sea un agregador).
- En un entorno de Gestión Central, una línea base generada en una unidad gestionada se creará utilizando únicamente los datos de dicha unidad, pero la línea base se almacenará en el Gestor central y estará disponible para su uso en cualquier otra unidad.
- En un entorno de Gestión Central, para generar una única línea base a partir de varias unidades gestionadas, la línea base se puede crear con datos del primer dispositivo gestionado y, a continuación, se puede fusionar utilizando los datos de los otros dispositivos, uno cada vez.

Acerca de las reglas sugeridas

Cuando se incluye una línea base en una política, el Creador de políticas puede generar reglas sugeridas a partir de la línea base. Generará el número mínimo de reglas necesarias para representar todo lo que se incluye en la línea base. A continuación, puede aceptar cualquiera o todas las reglas sugeridas, y modificar las aceptadas según sea necesario. Además de ser una forma cómoda de generar una política explícita (en lugar de una política implícita basada únicamente en una línea base), este es un paso importante para validar que una línea base no incluye actividades erróneas o maliciosa que pudiesen haberse producido durante el periodo de la línea base.

Es posible que desee modificar las reglas sugeridas si descubre una actividad que se ha producido durante el periodo de la línea base que desearía supervisar o de la que desearía ser alertado en el futuro. Simplemente adaptaría la regla sugerida adecuada desde la línea base y le asignaría la acción deseada. De forma predeterminada, las reglas sugeridas se colocarán antes de la regla de línea base, de modo que la acción especificada se seguirá antes de que se ejecute la regla de línea base para permitir ese mandato sin ninguna prueba de reglas adicional.

Nota: El Creador de políticas también puede generar reglas a partir de la ACL de la base de datos. Consulte Políticas para obtener más información.

Acerca de los grupos de objetos sugeridos

Al generar reglas sugeridas a partir de la línea base o desde la ACL (lista de control de acceso) de la base de datos, el Creador de políticas minimiza el número de reglas sugeridas creando grupos de objetos sugeridos. Por ejemplo, supongamos que la línea base incluye un mandato determinado que sólo hace referencia a tres objetos: AAA, BBB y CCC, y que todavía no se ha definido un grupo de objetos que conste únicamente de estos tres objetos. El Creador de políticas creará un grupo de objetos sugeridos para dichos objetos y generará una única regla para el mandato, que hará referencia al grupo de objetos sugeridos.

Puede visualizar la pertenencia a un grupo de objetos sugeridos y la opción de aceptar o rechazar cada grupo. En el ejemplo que se acaba de proporcionar, si rechaza el grupo de objetos sugeridos, la única regla que hace referencia al mismo se sustituirá por tres reglas sugeridas (una cada para objeto AAA, BBB y CCC).

Creación de una línea base

1. Pulse Proteger > Políticas de seguridad > Creador de línea base para abrir el Buscador de líneas base.
2. Pulse Nuevo para abrir el Creador de línea base.
3. Especifique un nombre de línea base exclusivo en el recuadro Descripción de línea base. No incluya caracteres de apóstrofo en la descripción de la línea base.

4. En el panel Sensibilidad de línea base, marque cada elemento en el que la línea base será sensible. Cuanto más sensible sea la línea base, más complejo será realizar las pruebas al crear la línea base y, más importante aún, al inspeccionar el tráfico. Consulte la Visión general, para obtener más información sobre la sensibilidad de las líneas base.
5. En el panel Umbral de línea base, especifique el número mínimo de apariciones para un mandato durante el periodo de la línea base para que dicho mandato se incluya en la línea base. Si se marcan uno o más recuadros de sensibilidad, este recuento se aplica a la combinación de los valores de sensibilidad.

   Si el enfoque que toma para la creación de la política de seguridad es la de permitir siempre los mandatos emitidos más comúnmente en el pasado, establezca este número por lo alto en el nivel adecuado. Si, por otro lado, desea asegurarse de que la línea base es exhaustiva, establezca este valor en 1. En cualquiera de los dos casos, puede hacer que el Creador de políticas sugiera reglas desde la línea base. Las reglas sugeridas se clasifican en orden descendente por frecuencia en el periodo de la línea base, de modo que puede decidir en ese momento si se deben incluir o modificar las reglas para cada mandato único emitido.

6. Utilice el panel de Información de red de línea base para identificar los clientes y los servidores que se deben incluir en la línea base. El método utilizado para seleccionar las direcciones IP a utilizar para construir la línea base es la misma para los servidores que para los clientes.

   Para cada dirección encontrada en los datos de línea base, primero se tiene en cuenta la pertenencia a un grupo codificado opcional. Un grupo codificado es una lista específica de direcciones IP para las que se generarán construcciones de línea base. Si se selecciona un grupo codificado, y si se encuentra una dirección IP en los datos de línea base se incluye en el correspondiente grupo codificado, dicho elemento se incluirá en la línea base para esa dirección IP específica. Por ejemplo, supongamos que se selecciona el grupo de IP de cliente codificado denominado ZoneAGroup y que dicho grupo incluye la dirección de cliente 192.162.14.33. Si el creador de la línea base encuentra el mandato SELECT abc FROM xyz desde dicha dirección IP, dicho mandato se contará para dicha dirección específica.

   Por el contrario, si no se selecciona ningún grupo codificado, o si se encuentra una dirección IP en los datos de la línea base que no son miembros del grupo seleccionado, ese mandato se puede contar con mandatos idénticos desde otras direcciones IP tal como indique la máscara de red correspondiente.

   La máscara de red es necesaria para agrupar tanto las direcciones IP del servidor como las del cliente. Las opciones incluyen todas las variaciones diferentes de las máscaras de subred entre 255.255.255.255 (deben coincidir los cuatro octetos) y 0.0.0.0 (todos los octetos pueden ser cualquier valor).

   Siempre debe:

   - Especificar una máscara de subred en el recuadro Máscara de red de servidor.
   - Especificar una máscara de subred en el recuadro Máscara de red de cliente.

   Para ilustrar cómo el creador de línea base utiliza máscaras de red para agrupar direcciones, supongamos que:
   - La máscara de red de cliente es 255.255.0.0, lo que significa que los dos primeros octetos deben coincidir, mientras que los dos octetos restantes pueden ser cualquier valor.
   - En los datos de línea base, se encuentra una solicitud con la dirección IP 192.168.3.211.
   - Dicha dirección IP de cliente no está en el grupo de IP de cliente codificado (o no hay seleccionado ningún grupo de IP de cliente codificado).
   - El mandato es SELECT abc FROM xyz.

   Al generar la línea base, este mandato se incluirá en el recuento de mandatos SELECT abc FROM xyz para todas las direcciones de IP de cliente de la subred 192.168.0.0.

7. Pulse Guardar para la comprobación de la validez y para guardar la definición de la línea base. Si ha omitido campos necesarios o ha especificado valores no válidos, la definición no se guardará y deberá resolver los problemas antes de intentar guardarla de nuevo.
8. Opcionalmente, pulse Roles para asignar roles a la política.
9. Opcionalmente, pulse Comentarios para añadir comentarios a la definición.
10. Después de que una línea base se haya guardado correctamente, los paneles Generación de línea base y Registro de línea base aparecerán en el panel.
11. Pulse en cualquier lugar del título del panel Generación de línea base para expandir el panel.
12. Proporcione las fechas Desde y Hasta para definir el periodo de tiempo desde el que se va a generar la línea base. Existen varias maneras de especificar fechas. Para obtener más información, consulte Fechas e indicaciones de fecha y hora. Independientemente de cómo especifique las fechas, se ignorarán los minutos y segundos.
13. Pulse el botón Generar para generar la línea base. Si ha modificado la definición de línea base, se le solicitará que guarde la definición antes de generar la línea base.

Nota: Después de generar satisfactoriamente la línea base por primera vez, se visualizarán campos adicionales en el panel Generación de línea base. Estos campos permiten fusionar datos de periodos de tiempo adicionales en la línea base, y para restringir las direcciones IP de servidor y cliente utilizadas durante cada periodo de tiempo adicional.

Fusión de información de línea base

Para fusionar información de línea base (para incluir información de periodos de tiempo adicionales y/o de distintos grupos de clientes y servidores, por ejemplo):

1. Pulse Proteger > Políticas de seguridad > Creador de línea base para abrir el Buscador de líneas base.
2. En la lista de Definición de línea base, seleccione la línea base en la que se va a fusionar la información de la línea base adicional.
3. Pulse Modificar para abrir el panel Editar línea base.
4. No modifique las selecciones de Sensibilidad de línea base. Si modifica la sensibilidad de la línea base, se le solicitará que genere una línea base completamente nueva para sustituir a la existente.
5. Opcional. Establezca el valor del Número mínimo de apariciones para añadir a la línea base en el panel Umbral de línea base. El valor especificado aquí no tiene ningún impacto en la información incluida anteriormente en la línea base. Una vez se añada algo a la línea base, no se eliminará durante la operación de fusión.
6. Opcional. Especifique información de red alternativa en el panel de Información de red de línea base. Los valores visualizados son los de la última operación de generación o fusión. Si la información fusionada proviene del mismo conjunto de servidores y/o clientes, deje estos campos sin modificar. De lo contrario, realice los cambios adecuados en este panel para seleccionar el tráfico que se debe incluir en la línea base.
7. Pulse en cualquier lugar del título del panel Generación de línea base para expandir el panel.
8. Proporcione las fechas Desde y Hasta para definir el periodo de tiempo desde el que se va a generar la línea base. Existen varias maneras de especificar fechas. Para obtener más información, consulte Fechas e indicaciones de fecha y hora. Independientemente de cómo especifique las fechas, se ignorarán los minutos y segundos.
9. Seleccione el botón de selección Fusionar.
10. Opcional. En el panel Selección de filtro, limite la generación de la línea base a direcciones IP de servidor y/o cliente específicas especificando una dirección IP seguida de una máscara de red. Por ejemplo, para seleccionar las direcciones IP de cliente desde la subred 192.168.9.x, especifique 192.168.9.1 en el primer recuadro de IP de cliente, y 255.255.255.0 en el segundo recuadro. Para incluir direcciones adicionales, pulse el botón Añadir y, a continuación, especifique la información de direcciones adicional.
11. Pulse Generar para generar la línea base. Si ha modificado la definición de línea base, se le solicitará que guarde la definición antes de generar la línea base.

Modificación de una línea base

Precaución: Antes de modificar una definición de una línea base, asegúrese de que comprende las implicaciones de modificarla, especialmente si la línea base cuya definición desea modificar y volver a generar se utiliza en una política instalada. Si modifica y vuelve a generar una línea base contenida en una política instalada, cuando vuelva a instalar esa política, ésta utilizará la nueva línea base. Para proporcionar una opción de reserva para las líneas base utilizadas por las políticas instaladas, considere en su lugar la clonación de estas líneas base y políticas, y la modificación y generación de las definiciones clonadas. Consulte Clonación de una línea base para obtener más información.

1. Pulse Proteger > Políticas de seguridad > Creador de línea base para abrir el Buscador de líneas base.
2. En la lista de Definición de línea base, seleccione la línea base que desea modificar. Pulse el botón Modificar para abrir el panel Editar línea base. Aparte del título del panel, este panel es idéntico al del panel Añadir línea base. Consulte Creación de una línea base para obtener instrucciones sobre cómo utilizar este panel.

Clonación de una línea base

Hay una serie de situaciones en las que es posible que desee definir una nueva línea base basada en una existente, sin modificar la definición original. Consulte el aviso de precaución.

1. Pulse Proteger > Políticas de seguridad > Creador de línea base para abrir el Buscador de líneas base.
2. En la lista de Definición de línea base, seleccione la línea base que desea clonar.
3. Pulse Clonar para abrir el panel Clonar línea base.
4. Especifique un nombre exclusivo para la nueva línea base en el recuadro Descripción de la nueva línea base. No incluya caracteres de apóstrofo en la descripción de la nueva línea base.
5. Para clonar las construcciones de línea base (los mandatos, básicamente) que se han generado para la línea base que se está clonando, marque el recuadro de selección Clonar construcciones.
6. Pulse Aceptar para guardar la nueva línea base. A continuación, puede abrir y editar la nueva línea base utilizando el Buscador de líneas base.

Eliminación de una línea base

1. Pulse Proteger > Políticas de seguridad > Creador de línea base para abrir el Buscador de líneas base.
2. En la lista de Definición de línea base, seleccione la línea base que desea eliminar.
3. Pulse Suprimir. Se le solicitará que confirme la acción.

Tema principal: Protección

Políticas

Una política de seguridad contiene un conjunto ordenado de reglas que se deben aplicar al tráfico observado entre servidores y clientes de base de datos. Cada regla se puede aplicar a una solicitud desde un cliente o a una respuesta desde un servidor. Se pueden definir varias políticas y se pueden instalar varias políticas en un dispositivo Guardium al mismo tiempo.

Cada regla en una política define una acción condicional. La condición probada puede ser una prueba simple, por ejemplo, se podrían comprobar los accesos desde una dirección de IP de cliente que no perteneciese a un grupo de direcciones IP de clientes autorizados. O bien, la condición probada podría ser una prueba compleja que considerase varios mensajes y atributos de sesión (usuario de base de datos, programa fuente, tipo de mandato, hora del día, etc.), y que podría ser sensible al número de veces que la condición se cumple dentro de un marco temporal especificado.

La acción desencadenada por la regla puede ser una acción de notificación (por ejemplo, un correo electrónico a uno o más destinatarios, por ejemplo), una acción de bloqueo (desconexión de la sesión de cliente) o el suceso podría simplemente registrase como una infracción de política. Se pueden desarrollar acciones personalizadas para realizar las tareas necesarias para las condiciones que pueden ser únicas para una aplicación o entorno dado. Para obtener una lista completa de acciones, consulte Visión general de acciones de reglas.

Se registra una infracción de política cada vez que se desencadena una acción de sólo registro o de alerta. Opcionalmente, el SQL que desencadena la regla (incluidos los valores de los datos) se pueden registrar con la infracción de la política. Las infracciones de política se pueden asignar a incidencias, ya sea automáticamente por un proceso o manualmente por parte de usuarios autorizados (consulte el separador Gestión de incidencias en la interfaz gráfica de usuario de Guardium). Para obtener más información, consulte Gestión de incidencias.

Nota: También se pueden grabar las alertas de correlación en el dominio de infracciones de política (consulte Alertas de correlación).

Además de registrar las infracciones, las reglas de política pueden afectar al registro del tráfico de cliente, que se registra como construcciones y como instancias de construcción.

- Las construcciones son básicamente prototipos de solicitudes que detecta Guardium en el tráfico. Las combinaciones de mandatos, objetos y campos incluidos en una construcción pueden ser muy complejas, pero cada construcción representa básicamente un tipo muy específico de solicitud de acceso. La detección y el registro de las nuevas construcciones empieza cuando se inicia el motor de inspección y, de forma predeterminada, continúa (excepto tal como se ha descrito), independientemente de las reglas de política de seguridad.
- También se registra cada instancia de una construcción detectada en el tráfico y cada instancia se relaciona con una sesión de cliente-servidor específica. No se almacena ningún SQL para una instancia de construcción, excepto cuando una regla de política solicita el registro de SQL para esa instancia, o para una sesión de cliente/servidor determinada de instancias (con o sin valores).

Además de controlar la inclusión de SQL en las instancias de construcción de cliente, una regla de política de seguridad puede inhabilitar el registro de las instancias y construcciones para el resto de una sesión.

En situaciones de gran volumen, el análisis y la agregación de información en construcciones e instancias se puede diferir utilizando la opción Log Flat. Cuando se utilice, la producción de alertas e informes se retrasará hasta que la información registrada se haya agregado. Consulte Registro para proceso Flat más adelante en este tema.

Para controlar completamente el tráfico del cliente que se registra, se puede definir una política como una política de seguimiento de auditoría selectiva. En ese tipo de política, las reglas de sólo auditoría y un patrón opcional identifican todo el tráfico del cliente para ser registrado. Consulte Utilización del seguimiento de auditoría selectivo más adelante en este tema.

Además de la instalación de nuevas políticas desde la pantalla Instalador de políticas de la Consola de administración/Instalación de políticas:

- Se puede instalar una nueva política desde la pantalla del Buscador de políticas.
- En la pantalla Definición de política, se puede volver a instalar una política instalada, sin tener que volver a instalar otras políticas instaladas.
- Desde la pantalla Reglas de política, se puede volver a instalar una regla de política instalada, sin volver a instalar toda la política.

Únicamente en una nueva instalación (no en actualizaciones), existe una política predeterminada. No tiene reglas y Auditoría selectiva está seleccionada (esto significa que el sistema Guardium no recopilará ningún tráfico por la política predeterminada). La política predeterminada en una versión de 64 bits de Guardium (instalación nueva) es de forma predeterminada - Ignorar actividad de datos para conexiones desconocidas.

Conceptos básicos de reglas de política

Dentro de una política, las reglas se evalúan en el orden en el que aparecen, a medida que se analiza cada elemento del tráfico.

Existen tres tipos de reglas:

- Una regla de acceso se aplica a las solicitudes de cliente; por ejemplo, podría comprobar mandatos UPDATE emitidos desde un grupo específico de direcciones IP.
- Una regla de excepción evalúa las excepciones devueltas por el servidor (respuestas); por ejemplo, sería posible comprobar cinco errores de inicio de sesión en un minuto.
- Una regla de extrusión evalúa los datos devueltos por el servidor (en respuesta a solicitudes); por ejemplo, podría comprobar los datos devueltos para detectar patrones numéricos que podrían ser números de la seguridad social o de tarjetas de crédito.

Categoría, clasificación y gravedad

Con cada regla, se puede asignar una categoría y/o una clasificación opcional. Se utilizan para agrupar infracciones de política para la gestión de indicendcias y la creación de informes.

Recuentos mínimos e intervalo de restablecimiento

Algunas actividades son normales y aceptables cuando se producen por debajo de una frecuencia dada. Pero estas mismas actividades podrían ser de interés cuando su frecuencia superase un umbral de tolerancia. Por ejemplo, si se permite el acceso a una base de datos interactiva, se podría esperar un frecuencia constante pero relativamente baja de anomalías de inicio de sesión, mientras que una frecuencia abruptamente elevada podría indicar que se está llevando a cabo un ataque.

Para tratar con umbrales, se puede especificar un recuento mínimo y un intervalo de restablecimiento para cada regla de política. Esto se puede utilizar, por ejemplo, para desencadenar la acción de regla después de que el recuento de anomalías de inicio de sesión supere 100 (el recuento mínimo) en un minuto (el intervalo de restablecimiento). Si se omite, la acción predeterminada es ejecutar la acción de regla cada vez que se satisfaga la regla.

Continuar en la siguiente regla

De forma predeterminada, la evaluación de las reglas de excepción y de acceso para una unidad de tráfico finaliza cuando se desencadena una regla, siempre que no haya varias acciones en una regla. En los casos en los que es necesario realizar varias acciones para las mismas condiciones o similares, marque el recuadro Continuar en la siguiente regla para dicha regla.

Nota: Continuar en la siguiente regla se aplica a las reglas de acceso que sigan a las reglas de acceso y a las reglas de excepción que sigan a las reglas de excepción, pero no a una regla de excepción que siga a una regla de acceso ni una regla de acceso que siga a una regla de excepción.

Las reglas de extrusión se procesarán independientemente del final de una regla de excepción o de acceso que preceda a la regla de extrusión. Consulte revocar reglas de extrusión en la tabla de Referencia de definiciones de regla al final de este tema para obtener información sobre la exclusión del registro de una respuesta que ya ha sido seleccionada para ser registrada por una regla anterior en la política.

Grabación de valores con infracción de política

Cuando se marca, la construcción real que hace que se satisfaga la regla se registrará en el atributo de serie SQL y estará disponible en los informes. Si no se marca, no se registrará ninguna sentencia SQL. Para incluir los valores completos en la infracción de política, marque el recuadro Registrar valores para dicha regla.

Nota: El SQL completo con valores sólo estará disponible en el registro de infracción de política, dentro del dominio de informes de infracciones de política. No estará disponible en el registro de tráfico del cliente ni en los informes procedentes del dominio de acceso a datos. Para incluir el SQL completo (con o sin valores de datos) en el registro de tráfico de red, utilice las acciones de regla Registrar SQL completo.

Para obtener más información sobre cómo trabajar con reglas, consulte los siguientes temas:

- Visualización de reglas de política para la política instalada
- Especificación de valores y/o grupos de valores en reglas
- Filtración de reglas para visualizar solo un subconjunto
- Copia de reglas
- Utilización de reglas sugeridas de la ACL de la base de datos.
- Adición o edición de reglas
- Utilización del Simulador de políticas

Especificación de valores y/o grupos de valores en reglas

Con muchos atributos de regla, es posible especificar un valor de grupo y/o un valor individual, mediante controles como, por ejemplo, los ilustrados para el usuario de la aplicación.

Tenga en cuenta que un miembro de grupo puede contener caracteres comodín (%), de forma que cada miembro de un grupo puede coincidir con varios valores reales.

Cuando se selecciona un grupo, tenga en cuenta que es posible que el grupo contenga comodines.

- **Regla negativa**: Marque el recuadro No para crear una regla negativa; por ejemplo, no el usuario de aplicación especificado, no ningún miembro del grupo seleccionado, o ni el usuario de aplicación seleccionado ni miembros del grupo seleccionado.
- Valor vacío: Especifique el valor especial guardium://empty para comprobar un valor vacío en el tráfico. Solo se permite en los siguientes campos: Nombre de BD, Usuario de BD, Usuario de aplicación, Usuario de SO, Aplicación origen, Tipo de suceso, Nombre de usuario de suceso y Texto de suceso de aplicación.
- Para definir un nuevo grupo para probarlo: Pulse en el botón Grupos para definir un nuevo grupo y, a continuación, seleccionar este grupo en la lista de Grupos.
- Para hacer coincidir con cualquier valor: Deje el recuadro de valor en blanco y no seleccione nada en la lista de Grupos (asegúrese de que se selecciona la línea de guiones, como en el ejemplo).
- Para hacer coincidir con un valor específico: Especifique ese valor en el recuadro de valor y no seleccione nada en la lista de Grupos.
- Para hacer coincidir con cualquier miembro de un grupo: Deje el recuadro de valor en blanco y seleccione el grupo en la lista. Si el recuento mínimo es mayor que 1, habrá un único contador, que se incrementará cada vez que haya un miembro del grupo que coincida.

- Para hacer coincidir un valor individual o cualquier miembro de un grupo: Especifique un valor específico en el recuadro de valor y seleccione un grupo de la lista. Si el recuento mínimo es mayor que 1, habrá un único contador, que se incrementará cada vez que haya un valor individual o un miembro del grupo que coincida.
- Si el recuento mínimo es mayor que 1, contar cada valor individual de forma separada: Especifique un punto (.) en el recuadro de valor y no seleccione nada de la lista de grupos. Tenga en cuenta que la opción del punto no se puede utilizar para los recuadros de Nombre de servicio ni Protocolo de red. Si el recuento mínimo es mayor que 1, contar cada miembro de un grupo forma separada: Especifique un punto (.) en el recuadro de valor y seleccione un grupo de la lista. Tenga en cuenta que la opción del punto no se puede utilizar para los recuadros de Nombre de servicio ni Protocolo de red.

Coincidencia de patrón utilizando expresiones regulares

Además de las pruebas de patrón especiales, se pueden utilizar expresiones regulares para buscar en el tráfico patrones complejos en los datos. La implementación de Guardium de expresiones regulares satisface el estándar POSIX 1003.2, que es distinto de la implementación de UNIX de expresiones regules. Se permiten expresiones regulares en cualquier campo que vaya seguido del botón Crear expresión regular.

Nota: También se pueden utilizar expresiones regulares en los siguientes campos (Usuario de BD, Usuario de aplicación, Aplicación de origen, Nombre de campo, Objeto, Valores de suceso de aplicación) escribiendo el valor especial guardium://regexp/(expresión regular) en el recuadro de texto que corresponde al campo.
Nota: IBM Security Guardium no da soporte a expresiones regulares para idiomas distintos del inglés.
Para obtener información detallada sobre cómo utilizar expresiones regulares, consulte Expresiones regulares.

- Pruebas de patrones especiales
  Puede utilizar estas pruebas de patrón especiales para identificar datos confidenciales que están contenidos en el tráfico que fluye entre servidor de base de datos y el cliente.
- Acciones de regla
  Hay una serie de factores a tener en cuenta cuando se selecciona la acción que se debe llevar a cabo cuando se satisface una regla.
- Creación de políticas
  Además de crear políticas, puede modificar, clonar o eliminar una política.
- Instalación de políticas
  Utilice este tema para instalar políticas en el recopilador de Guardium y para modificar la planificación.
- Campos de definición de regla
  Puede utilizar estos campos al definir reglas de política.
- Integración de reglas personalizadas con políticas de Guardium
  Este tema muestra cómo modificar/derivar automáticamente políticas de Guardium desde un sistema de titularidad personalizado.
- Utilización de la acción Ignorar adecuada
  En este tema se explica cómo se manejan los datos al utilizar acciones de Ignorar en reglas de política.
- Conjuntos de caracteres
  Los códigos de los conjuntos de caracteres se utilizan en las reglas de extrusión.

Tema principal: Protección

Pruebas de patrones especiales

Puede utilizar estas pruebas de patrón especiales para identificar datos confidenciales que están contenidos en el tráfico que fluye entre servidor de base de datos y el cliente.

Cada regla de política puede incluir una prueba de patrón especial individual. Para utilizar una de estas pruebas, haga que el nombre de la regla empiece con uno de los nombres de prueba de patrón especiales, seguido de un espacio y uno o más caracteres adicionales para hacer que el nombre de regla sea exclusivo. Por ejemplo, si está buscando números de Seguridad Social de sus empleados, podría denominar la regla como `guardium://SSEC_NUMBER employee`. Adicionalmente puede especificar todos los demás componentes de la regla, como por ejemplo direcciones IP de servidor y de cliente específicas.

Estas pruebas identifican patrones de caracteres, que no garantizan que se haya encontrado realmente el elemento buscado como, por ejemplo, el número de la Seguridad Social. Puede haber falsos positivos por diversas circunstancias, especialmente si hay concatenadas secuencias extensas de valores numéricos en los datos.

guardium://CREDIT_CARD

Detecta patrones de números de tarjeta de crédito. La prueba busca una serie de 16 dígitos o de cuatro conjuntos de cuatro dígitos, con cada conjunto separado por un espacio en blanco. Esta prueba de patrón especial también funciona con patrones de números de tarjeta de crédito de 15 dígitos de American Express (primer dígito 3 y segundo dígito, 4 o 7). Por ejemplo: `1111222233334444` o `1111 2222 3333 4444`

Cuando un nombre de regla empieza por "guardium:// CREDIT_CARD", y existe un patrón de número de tarjeta de crédito válido en el campo Patrón de datos, la política utiliza el algoritmo Luhn, un algoritmo ampliamente utilizado para validar números de identificación como, por ejemplo, de tarjeta de crédito, además de la coincidencia de patrón estándar. El algoritmo de Luhn es una comprobación adicional y no reemplaza la comprobación de patrón. Un número de tarjeta de crédito válido es una serie de 16 dígitos o cuatro conjuntos de cuatro dígitos, separados por un espacio en blanco. Existe un requisito de tener el nombre de regla guardium://CREDIT_CARD y un número [0-9]{16} válido en el recuadro Expresión de búsqueda para implicar el algoritmo de Luhn en esta coincidencia de patrón.

guardium://PCI_TRACK_DATA

Detecta dos patrones de datos de banda magnética. El primer patrón consta de un punto y coma (;), 16 dígitos, un signo igual (=), 20 dígitos y un signo de interrogación (?), como por ejemplo:

```
;1111222233334444=11112222333344445555?
```

El segundo patrón consta de un signo de porcentaje (%), el carácter B, 16 dígitos, un signo de intercalación (^), una serie de caracteres de longitud variable terminada por una barra inclinada (/), una segunda serie de caracteres de longitud variable terminada por un símbolo de intercalación (^), 31 dígitos y un signo de interrogación (?), como por ejemplo:

```
%B1111222233334444^xxx/xxxx x^11112222333344445555666677778888?
```

guardium://SSEC_NUMBER

Detecta números en formato de número de la Seguridad Social: tres dígitos, guion (-), dos dígitos, guión (-) y cuatro dígitos, como, por ejemplo, `123-45-6789`. Los guiones son necesarios.

guardium://CPF

Cadastro de Pessoas Físicas (CPF), un identificador personal de Brasil. Contiene 11 dígitos con el formato `nnn.nnn.nnn-nn`, donde los dos últimos son dígitos de comprobación. Los dígitos de comprobación se calculan a partir de los nueve dígitos originales para proporcionar la verificación de que el número es válido. El

formato de los caracteres dentro de la expresión es opcional. Si hay una coincidencia en la expresión, se validan los dígitos de comprobación.

guardium://CNPJ

Cadastro Nacional de Pessoas Jurídicas (CNPJ), número de identificación utilizado por las empresas en Brasil. Contiene 14 dígitos con el formato `00.000.000/0001-00` donde:

- Los primeros ocho números indican el registro.
- Los cuatro números siguientes identifican la oficina de la entidad. 0001 es el valor predeterminado de la sede central.
- Los 2 últimos números son los dígitos de comprobación.

El formato de los caracteres dentro de la expresión es opcional. Si hay una coincidencia en la expresión, se validan los dígitos de comprobación.

Tema principal: Políticas

Acciones de regla

Hay una serie de factores a tener en cuenta cuando se selecciona la acción que se debe llevar a cabo cuando se satisface una regla.

Acciones de bloqueo (S-TAP/S-GATE)

Esta sección describe las acciones Terminar S-TAP y S-GATE.

Acción Terminar S-TAP

La acción TERMINAR S-TAP terminará una conexión de una base de datos (una sesión) e impedirá solicitudes adicionales en dicha sesión. Esta acción está disponible en S-TAP, independientemente de si se utiliza S-GATE.

Nota: Con TERMINAR S-TAP, normalmente la solicitud de desencadenamiento no será bloqueada, pero si se bloquearán las solicitudes adicionales de dicha sesión (con una probabilidad elevada, a veces puede discurrir más de una solicitud antes de que se termine la sesión).

Acciones de S-GATE

S-GATE proporciona protección de base de datos a través de S-TAP tanto para conexiones locales como de red.

Cuando S-GATE está disponible, todas las conexiones (sesiones) de base de datos se evalúan y codifican para supervisarse en una de las siguientes modalidades S-GATE:

- Conectado (Attached) (S-GATE está "activado") – S-TAP está en modalidad de cortafuegos para esa sesión, aloja las solicitudes de base de datos y espera un veredicto en cada solicitud antes de liberar sus respuestas. En esta modalidad, hay latencia. Sin embargo, se asegura que se bloquearán las solicitudes inesperadas.
- Desconectado (Detached) (S-GATE está "inactivo") - S-TAP está en modalidad de supervisión normal para dicha sesión, pasa solicitudes al servidor de bases de datos sin ningún retardo. En esta modalidad no debería haber latencia.

La configuración de S-GATE en "guard_tap.ini" define la modalidad de S-GATE predeterminada ("attached" o "detached") para todas las sesiones, así como otros valores predeterminados relacionados con los veredictos de S-GATE cuando el recopilador no está respondiendo. Además de la configuración S-GATE predeterminada, S-GATE se controla mediante el mecanismo de política en tiempo real utilizando las siguientes acciones de regla de política S-GATE:

- CONECTAR S-GATE: establece la modalidad S-GATE en conectado ("Attached") para una sesión específica.

  El propósito es utilizar esta característica cuando se cumple un determinado criterio que eleve la necesidad de observar (y si es necesario, bloquear) el tráfico en dicha sesión.
- DESCONECTAR S-GATE: establece la modalidad S-GATE en desconectado ("Detached") para una sesión específica.

  El propósito es utilizar esta característica en sesiones consideradas como "seguras" o sesiones que no admiten latencia.
- TERMINAR S-GATE: Tiene efecto únicamente cuando la sesión está conectada ("Attached"). Descarta la respuesta de la solicitud del cortafuegos, lo provocará la finalización de la sesión en algunas bases de datos. La regla de política TERMINAR S-GATE provocará la terminación de una sesión observada anteriormente.

Nota:

- La terminación de S-GATE/ S-TAP no funciona en un grupo de IP de cliente cuyos miembros tengan caracteres comodín. La terminación S-GATE/S-TAP sólo funciona con una única dirección IP. Los grupos deben manejar comodines si el cliente desea utilizar varias entradas de IP. El cliente puede crear grupos de clientes/usuarios de confianza/de no confianza para manejar sus necesidades empresariales en las políticas.
- Con A-TAP y S-GATE, hay limitaciones con los kernels inferiores de Linux. Básicamente, para S-TAP 10.1.2 y superior, S-GATE está soportado excepto con Linux con ATAP y kernels inferiores a 2.6.36.
- Con bases de datos MySQL, debe tenerse en cuenta que la conexión de línea de mandatos predeterminada de MySQL es 'mysql -u<user> -p<pass> <dbname>'

  En esta modalidad, MySQL primero correlacionará todos los objetos y campos de esta base de datos para dar soporte a la cumplimentación automática (con el tabulador). Cuando haya una regla de terminación en cualquier objeto o campo involucrado en esta correlación, inhabilitará la sesión de conexión forma inmediata. Para evitar esto, conéctese a MySQL con el distintivo "-A", que inhabilitará la característica "' auto-complete" y no desencadenará la regla "terminate". Otra opción es un ajuste de forma que la regla no termine en ningún acceso a estos objetos/campos y en su lugar encuentre un criterio que sea más preciso y no desencadene la regla en la secuencia de inicio de sesión.

Acciones de alerta

Las acciones de alerta envían notificaciones a uno o más destinatarios.

Para cada acción de alerta, se pueden enviar varias notificaciones. Las notificaciones pueden ser una combinación de uno o varios de los tipos de notificación siguientes:

- Mensajes de correo electrónico, que deben direccionarse a los usuarios de Guardium, y que se enviarán a través del servidor SMTP configurado para Guardium. Destinatarios adicionales para la notificación de correo electrónico en tiempo real son el invocador (el usuario que ha iniciado el mandato SQL real que ha provocado el desencadenante de la política) y el propietario (el propietario o propietarios de la base de datos). El invocador y el propietario se identifican mediante la recuperación de los ID de usuario (basados en IP) configurados mediante las API de Guardium. La opción Asociación de base de datos - usuario de seguridad de datos (disponible desde accessmgr) visualiza la correlación (es similar a lo que se visualiza si se ejecuta el mandato de API de Guardium "list_db_user_mapping").
- Condiciones de excepción SNMP, que se enviarán a la comunidad de condiciones de excepción configurada para el dispositivo Guardium.

- Mensajes syslog, que se escribirán en el syslog.
- Notificaciones personalizadas, que son manejadores de notificaciones escritos por el usuario, implementados como clases de Java™.

Nota: La definición de las alertas y las notificaciones no están sujetas a la seguridad de nivel de datos. Entre otras razones, se debe a que las alertas no se evalúan en el contexto del usuario, la alerta puede estar relacionada con bases de datos asociadas a varios usuarios y para evitar situaciones donde al final nadie recibe la notificación.

Las plantillas de mensaje se utilizan para generar alertas. Se crean y modifican varias plantillas de mensajes con nombre desde el perfil global. Hay varios tipos de acciones de alerta, cada una de las cuales puede ser adecuada para cada tipo de situación diferente.

- Alertar diariamente envía notificaciones sólo la primera vez que se cumple la regla cada día.
- Alertar una vez por sesión envía notificaciones sólo una vez por cada sesión en la que se cumple la regla. Esta acción puede ser adecuada en situaciones en las que desee saber que se ha producido un determinado suceso, pero no en cada instancia de dicho suceso durante una sesión individual. Por ejemplo, es posible que desee que se le envíe una notificación cuando se actualice un objeto importante determinado, pero si un programa actualiza miles de instancias de dicho objeto en una sola sesión, es casi seguro que no querrá que se envíen miles de notificaciones a los destinatarios de la alerta.

- Solo alerta - Con Solo alerta, con el tipo syslog, el mensaje va directamente a /var/log/messages. Con otros tipos de Solo alerta, el mensaje se enviará a la tabla MESSAGE. Solo alerta no notifica infracciones de la política.

- Alertar por coincidencia envía notificaciones cada vez que se satisfaga la regla. Esto sería lo adecuado para una condición que requiere atención cada vez que se produce.
- Alerta por granularidad de tiempo envía notificaciones una vez por periodo de granularidad de registro. Por ejemplo, si la granularidad de registro se establece en una hora, las notificaciones se enviarán solo para la primera coincidencia de la regla durante cada hora. (El administrador de Guardium establece la granularidad del registro en el panel Configuración del motor de inspección).

Acciones registrar o ignorar

Estas acciones controlan el nivel de registro, basándose en el tráfico observado.

Los mandatos de Registrar e Ignorar habitualmente siempre están disponibles, sin embargo, la acción Solo auditoría únicamente está disponible para una política de Seguimiento de auditoría selectivo. Las acciones permitidas para las reglas de acción, reglas de excepción y reglas de extrusión son diferentes. Pulse en el botón Añadir acción para ver las opciones.

- Solo auditoría: Disponible solo para la política de Seguimiento de auditoría selectivo. Registra la construcción que desencadenó la regla. Para una política de Seguimiento de auditoría selectivo, de forma predeterminada no se registran construcciones, de forma que utilice esta selección para indicar lo que debe registrarse. Cuando se utiliza la API de sucesos de aplicación, debe utilizar esta acción para forzar el registro de nombres de usuario de base de datos, si desea que dicha información esté disponible en los informes (de lo contrario en este caso, el nombre de usuario estará en blanco).
- Permitir: Cuando se cumpla, no registrar una infracción de política. Si se selecciona la acción "Permitir", no se puede añadir ninguna otra acción a la regla. Se registran las construcciones.
- Alerta y auditoría de FAM - dos acciones de regla - Alertar, con un suceso coincidente, desencadenar una alerta (utilizando receptor y plantilla) y Auditar, registrar la construcción que desencadenó la regla.
- Solo auditar FAM - registra la construcción que desencadenó la regla.
- Ignorar FAM - No registrar este suceso.
- Solo registrar infracciones de acceso FAM - registra infracciones de acceso FAM.
- Solo registrar - registrar solo la infracción de política. Nos referimos al hecho de que la regla se desencadenó como una infracción de política. A excepción de la acción Permitir, se registra una infracción de política cada vez que se desencadena una regla (a menos que dicha acción suprima el registro).
- Registrar detalles de enmascaramiento: Registra el SQL completo de esta solicitud, sustituyendo valores con interrogantes de cierre (???). Esta acción está disponible para reglas de acceso y reglas de extrusión.
- Registrar detalles completos: Registra la serie de SQL completa y la indicación de fecha y hora exacta de esta solicitud. Consulte las notas en Discusión adicional y ejemplos.
- Registrar detalles completos con valores: Como Registrar detalles completos, pero además, cada valor se almacena como un elemento separado (analiza y registra los valores en tablas independientes en la base de datos). Esta acción de registro utiliza más recursos del sistema puesto que registra valores específicos de los mandatos pertinentes. Utilice esta acción de registro únicamente cuando necesite generar informes con condiciones específicas en estos valores. La activación de esta opción de acción de registro no está disponible a no ser que consulte con los servicios técnicos (usuario administrador/Herramientas/Mantenimiento de soporte).
- Registrar detalles completos por sesión: Registra la serie de SQL completa y la indicación de fecha y hora exacta para esta solicitud y para el resto de la sesión.
- Registrar detalles completos con valores por sesión: Consulte las descripciones de Registrar detalles completos con valores y Registrar detalles completos por sesión. La activación de esta opción de acción de registro no está disponible a no ser que consulte con los servicios técnicos (usuario administrador/Herramientas/Mantenimiento de soporte).
- Omitir registro: Cuando haya una coincidencia, no registrar la infracción de política y detener el registro de las construcciones. Es similar a la acción Permitir, pero además detiene el registro de construcciones. Esta acción se utiliza para eliminar el registro de construcciones de solicitudes que se sabe que no son de interés. GDM_CONSTRUCT se registrará en algunos casos, porque el análisis/registro de la construcción tiene lugar antes de que se aplique la regla. Sin embargo, la construcción no se incluirá en la sesión. Esta característica también se aplica a las reglas de excepción relacionadas con solo códigos de error de base de datos, lo que permite a los usuarios no registrar errores cuando una aplicación genera grandes cantidades de errores y no hay nada que el usuario pueda hacer para detener los errores de aplicación.
- Ignorar respuestas por sesión: Se ignorarán respuestas para el resto de la sesión. Esta acción no registra una infracción de política, pero detiene el análisis de respuestas para el resto de la sesión. Esta acción es útil en los casos en los que sabe que la respuesta de la base de datos no será de interés. Esta acción funciona cuando se inspeccionan datos desde un S-TAP. Esta acción no funciona al inspeccionar datos desde un puerto SPAN.
  Nota: Para ignorar respuestas por sesión, puesto que el sniffer no recibe ninguna respuesta para la consulta o se ignora, entonces los valores para COUNT_FAILED y SUCCESS son el valor predeterminado para la tabla, en este caso COUNT_FAILED= 0 y SUCCESS=1.
- Ignorar sesión: Se ignora la solicitud actual y el resto de la sesión. Esta acción no registra una infracción de política, pero detiene el registro de las construcciones y no realizará pruebas para verificar infracciones de política de ningún tipo durante el resto de la sesión. Esta acción podría ser útil si, por ejemplo, la base de datos incluye una región de prueba, y no hay una necesidad de aplicar reglas de política en esa región de la base de datos. Las reglas de Ignorar sesión proporcionan el método más eficaz para filtrar el tráfico. Una regla de ignorar sesión provocará que la actividad de sesiones individuales sea descartada por el S-TAP o completamente ignorada por el sniffer. Nota: La información de conexión (inicio de sesión/fin de sesión) siempre se registra, incluso si se ignora la sesión.
- Ignorar sesión de S-TAP: Se ignorará la solicitud actual y el resto de la sesión S-TAP. Esta acción se realiza en combinación con la especificación en la pantalla del menú del creador de políticas de determinados sistemas, usuarios o aplicaciones que están produciendo un gran volumen de tráfico de red. Esta acción es útil en los casos en los que sabe que la respuesta de la base de datos de la sesión de S-TAP no será de interés. Hay dos opciones para Ignorar sesión de S-TAP: IGNORE_ENTIRE_STAP_SESSION - Se trata de una acción de ignorar "estricta" que no es posible revocar, e IGNORE_STAP_SESSION (REVOCABLE) - Se trata de una acción de ignorar "leve", puesto que esta acción de regla puede habilitar de nuevo el tráfico de la sesión para enviarse sin precisar de una nueva conexión a la base de datos. Nota para ignore_stap_session (revocable) - El mandato Revocar ignorar STAP es persistente para el host S-TAP en un proceso de sniffer. Las nuevas sesiones abiertas después de que el S-TAP se encuentra en el estado de ignorar revocado NO se ignorarán (incluso si se desencadena la regla IGNORAR SESIÓN S-

TAP (REVOCABLE). Revocar ignorar - Las sesiones que se ignoraron por la acción de "IGNORAR SESIÓN S-TAP (REVOCABLE)" se reanudarán, lo que significa que el tráfico se enviará al sistema Guardium después de que el S-TAP haya recibido el mandato "Revocar ignorar". (Este mandato se puede enviar desde Control S-TAP --> enviar mandato).

- Ignorar SQL por sesión: No se registrará SQL durante el resto de la sesión. Las excepciones se continuarán registrando, sin embargo, el sistema no capturará las series SQL que corresponden a las excepciones.
- Registrar contador de extrusión: Disponible sólo para reglas de extrusión, esta acción actualiza el contador, pero no registra los datos devueltos. Esta acción ahorra espacio de disco cuando el valor de contador es lo más importante y los valores devueltos tienen menos importancia.
- Registrar contador de extrusión enmascarado: Solo disponible para reglas de extrusión, esta acción actualiza el contador; registra la solicitud SQL, sustituyendo valores con cierre de interrogante; no registra los datos devueltos (respuesta).
- Cuarentena: Disponible para las reglas de acceso, excepción y extrusión, el objetivo de esta acción es impedir que el mismo usuario inicie sesión en el mismo servidor durante un periodo de tiempo determinado. Hay un elemento de validación: no puede tener una regla con una acción de CUARENTENA sin haber cumplimentado un valor con la cantidad de tiempo que el usuario estará en cuarentena. Consulte Cuarentena durante (minutos) para establecer este tiempo de cuarentena. Si la sesión está bajo observación (escenario S-GATE), envía un veredicto de descartar. Si la sesión no está bajo observación (escenario TERMINAR S-TAP), hace que el S-TAP detenga la sesión. Tome el tiempo actual y añádale el número de minutos del campo intervalo de restablecimiento. Obtendrá una nueva indicación de fecha y hora. En una nueva estructura mantendrá una lista ordenada (ordenada por esta indicación de fecha y hora). Cada elemento tiene, además de la indicación de fecha y hora, una IP de servidor, un tipo de servidor, un nombre de usuario de BD, un nombre de servicio y un distintivo que indica si se trata de una sesión observada o no.
- No analizar - No analizar la sentencia SQL.
- Análisis rápido sin campos - No analizar campos en la sentencia SQL. Todas las reglas de análisis rápido solo se aplican si la serie SQL tiene más de 100 caracteres.
- Análisis rápido nativo - Solo se utiliza para Guardium S-TAP for DB2 on z/OS. Utilice esta acción de regla en un entorno en el que el tráfico intenso esté sobrecargando el sniffer. El uso de esta acción de regla debe mejorar el rendimiento en S-TAP for DB2 on z/OS.
- Análisis rápido: Sólo para reglas de acceso, para el resto de la sesión, No analizar la sentencia SQL. Esta acción reduce el tiempo de análisis. En esta modalidad, se pueden determinar todos los objetos a los que se ha accedido (ya que los objetos aparecen antes de la cláusula WHERE), pero las instancias de objeto exactas afectadas serán desconocidas, ya que se determina mediante la cláusula WHERE.
- Redactar: Solo para reglas de extrusión, esta característica permite a un cliente enmascarar partes de la salida de la consulta de la base de datos (por ejemplo, números de tarjeta de crédito) en informes para determinados usuarios. La selección del Carácter de reemplazamiento en la sección Patrón de datos de las elecciones del menú de regla de extrusión define el carácter enmascaramiento. Cuando la salida de la regla de extrusión coincida con la expresión regular del Patrón de datos, las partes que coincidan con las subexpresiones entre paréntesis "(" y ")" serán reemplazadas con el carácter de enmascaramiento. También se pueden utilizar expresiones regulares predefinidas (expresiones regulares rápidas). Consulte Patrón de datos en Campos de definición de regla para obtener más información.
  Restricción:
  - La redacción no funciona en sesiones abiertas después de una actualización en directo de S-TAP.
  - La redacción no funciona en las tablas creadas con el tipo de número y campo.
  - No se da soporte al Patrón de SQL para reglas de redacción.
- Grabar valores de forma separada/ No grabar valores de forma separada: Esta acción se basa en una regla de acceso basada en sesión. Utilizada en la función Reproducir para distinguir entre transacciones.
- Marcar como confirmación automática ACTIVADA / Marcar como confirmación automática DESACTIVADA: Esta acción es una regla de acceso basada en una sesión. Se utiliza en la función Reproducir a consecuencia de varios modelos de confirmación automática para distintas bases de datos.
- Auditoría z/OS: Se utiliza específicamente para las reglas de política de Perfil de recopilación z/OS (IMS, conjuntos de datos y DB2), que se utilizan para especificar qué tráfico se debe recopilar en el servidor z/OS. Esta acción especifica que el tráfico que cumple con los criterios de filtro se envía al recopilador, y es la única acción que se puede especificar en una regla de Perfil de recopilación.

Nota:

La Redacción (limpieza) en Linux está soportada a partir de la versión 9.1. Para todas las plataformas de UNIX, la limpieza solo está soportada con conjuntos de caracteres ANSI.

Las reglas de redacción (limpieza) se deberían establecer a nivel de sesión (es decir, desencadenar reglas con atributos de sesión como, por ejemplo, direcciones IP, Usuarios, etc) y no a nivel / atributos de SQL (como, por ejemplo, OBJECT_NAME o VERB), puesto que si establece la regla de limpieza en SQL que es necesario limpiar, probablemente las instrucciones de limpieza tardarán algunos milisegundos en llevarse a cabo en el S-TAP donde algunos resultados podrían pasar sin enmascararse.

Para garantizar que se limpia todo el SQL, establezca la modalidad predeterminada de S-TAP (S-GATE) en "conectado" ("attach") para todas las sesiones (en guard_tap.ini). Esto garantizará que ningún mandato pase sin ser inspeccionado por el motor de reglas y cada solicitud será alojada a la espera del veredicto de la política con relación a la solicitud. Este despliegue introducirá algo de latencia, pero esta es la forma de garantizar la limpieza del 100% de los datos.

En el caso de la base de datos de Informix, cuando se utiliza char como tipo de datos, no habrá null como terminación al final de cada columna. Por lo tanto, las cuatro columnas se capturan en la llamada de sistema sendmsg como una entidad. KTAP siempre tratará de redactar los datos que captura. Se trata de una limitación al utilizar la redacción con la base de datos de Informix.

Nota:

Para el soporte HTTP, hay limitaciones de acciones de política. Las siguientes acciones de política no están soportadas para HTTP: Terminar S-TAP y Omitir registro.

Para otras acciones, HTTP no da soporte a lo siguiente:

- Ignorar respuestas por sesión: porque HTTP no da soporte a la excepción y a la extrusión.
- Ignorar SQL por sesión: porque HTTP no contiene SQL.
- Cuarentena: Esta acción se utiliza para poner en cuarentena al usuario, sin embargo, HTTP no da soporte a DBUser ni a OSUser.
- Análisis rápido: Esta acción es para registrar SQL.
- Terminar SGate: Esta acción no está soportada para Hadoop - todas las acciones de terminación no funcionan con HTTP.

Para condiciones de política - estas condiciones no están soportadas para HTTP:

MAC cliente; Nombre de BD; Usuario de BD; Usuario de aplicación; Usuario de SO; Aplic. origen; Patrón de máscara; Carácter de reemplazamiento; Minutos para la cuarentena; Umbral de registros afectados; Patrón XML; Tipo de suceso; Nombre de usuario de suceso; Texto de valores de suceso de aplicación; Grupo de texto de valores de suceso de aplicación; Grupo y texto de valores de suceso de aplicación; Numérico; Fecha.

Discusión adicional y ejemplos

Registrar detalles completos

De forma predeterminada, el recopilador de Guardium enmascara todos los valores al registrar una serie de SQL. Por ejemplo

```
insert into tableA (name,ssn,ccn) values ('Bob Jones', '429-29-2921','29249449494949494')
```

se registra como `insert into tableA (name,ssn,ccn) values (?, ?,?)`. Este es el comportamiento predeterminado por dos razones:

1. Los valores no se deberían registrar de forma predeterminada porque pueden contener información confidencial.
2. El registro sin valores proporciona un mayor rendimiento del sistema y una mayor retención de datos dentro del dispositivo. Muy a menudo, el tráfico de la base de datos consta de muchas solicitudes de SQL, idénticas en todo excepto por sus valores, que se repiten cientos, miles o incluso millones de veces por hora. Mediante el enmascaramiento de valores, Guardium es capaz de agregar estas solicitudes SQL en una única solicitud denominada "construcción". Cuando se registran las construcciones, en lugar de registrarse de forma separada cada construcción/solicitud de SQL, solo se registra una vez por hora (por sesión) con un contador con el número de veces que se ha ejecutado la construcción. Esto puede ahorrar una gran cantidad de espacio de disco porque, en lugar de crear cientos (o millones) de líneas en la base de datos, sólo se añade una línea nueva.

Con Registrar detalles completos, Guardium registra los datos con los valores sin enmascarar y cada solicitud. Registrar todos los detalles también proporcionan la indicación de fecha y hora exacta, mientras que el registro sin detalles proporciona la indicación de fecha y hora de la construcción más reciente dentro del periodo de tiempo de granularidad (normalmente 1 hora).

Ignorar sesión de S-TAP - Ignorar sesión de S-TAP hace que el recopilador envíe una señal a S-TAP indicándole que detenga el envío de todo el tráfico, con la excepción de la notificación de fin de sesión, para sesiones específicas. Por ejemplo, si tiene una regla que dice `where DBUserName?=scott, Ignore S-TAP Session`:

- Cuando Scott inicia una sesión en el servidor de base de datos, S-TAP envía la información de conexión al recopilador.
- El recopilador registra la conexión. La información de sesión (inicio de sesión/fin de sesión) siempre se registra.
- El recopilador envía una señal a S-TAP para que deje de enviar más tráfico desde esta sesión específica. Esto significa que los mandatos que Scott ejecute con relación al servidor de base de datos y sus respuestas (conjuntos de resultados, errores de SQL, etc.) que envíe el servidor de base de datos a Scott serán descartados por parte de S-TAP y nunca llegarán al recopilador.
- Cuando Scott finalice la sesión en el servidor de bases de datos, S-TAP enviará esta información al recopilador (siempre se realizará un seguimiento de la información de inicio/finalización de sesión incluso si se ignora la sesión).
- Cuando Scott vuelve a iniciar la sesión, estos pasos se repiten. Es el recopilador, y no el S-TAP, quien mantiene la lógica por la que se deben ignorar las sesiones.

Es importante tener en cuenta que las reglas de Ignorar sesión siguen siendo muy importantes para incluirlas en la política incluso si se utiliza un Seguimiento de auditoría selectivo. Las reglas de Ignorar sesión disminuyen considerablemente la carga en un recopilador al filtrar la información a nivel de S-TAP; el recopilador nunca la recibe y no tiene que consumir recursos analizando el tráfico que al final no se registra. Una política de Seguimiento de auditoría selectivo sin reglas de Ignorar sesión significaría que todo el tráfico se enviaría desde el servidor de base de datos al recopilador, lo que haría que el recopilador tuviese que analizar todos los mandatos y conjuntos de resultados generados por el servidor de base de datos.

Utilización de sentencias por lotes MS-SQL o Sybase en la aplicación Guardium

Limitación

La finalización correcta o con fallos de los mandatos SQL en las sentencias de lotes de MS-SQL o Sybase podría no mostrarse correctamente.

Las sentencias de lotes de MS-SQL o Sybase SQL se utilizan principalmente al crear procedimientos complejos.

Cuando se ejecutan sentencias SQL por separado, se sigue el estado de cada sentencia por separado y se tiene el valor de éxito o fracaso de las sentencias.

Cuando un se ejecuta conjuntamente un lote de sentencias SQL (utilizadas en MS-SQL o Sybase), el estado devuelto es el estado individual de la última transacción en el lote.

Ejemplo de Guardium

[Inicio de lote de SQL]

Sentencia SQL 1 - fallo

Sentencia SQL 2 - fallo

Sentencia SQL 3 - satisfactoria

[Fin de lote de SQL]

En la aplicación Guardium, solo se informa del éxito o fracaso de la última sentencia SQL de un lote de sentencias MS-SQL o Sybase. En este caso, se informa del éxito para la sentencia por lotes MS-SQL o Sybase, aunque hayan fallado las sentencias SQL 1 y SQL2.

Establecer conjunto de caracteres

Utilice una acción bajo una regla de extrusión de política para poder adjuntar conjuntos de caracteres alternativos para la sesión.

Reglas de patrón especiales con conjuntos de caracteres

Ejemplo de regla de extrusión (con hint):

Conjunto de caracteres EUC-JP (código 274).

Patrón de regla de extrusión: `guardium://char_set?hint=274`

Como resultado se adjunta una regla de extrusión a la sesión. El analizador utilizará EUC-JP en la sesión si no hay otro conjunto de caracteres.

Ejemplo de regla de extrusión (con force):

Conjunto de caracteres EUC-JP (código 274).

Patrón de regla de extrusión: `guardium://char_set?force=274`

Como resultado, se adjunta una regla de extrusión a la sesión y el analizador utilizará el juego de caracteres EUC-JP en cualquier caso. El juego de caracteres utilizado con anterioridad será sustituido por EUC-JP.

Tenga en cuenta que las reglas de extrusión suelen adjuntarse a la sesión con algún retardo. Por lo tanto, las sesiones cortas o el inicio de la sesión no reflejarán de forma inmediata el cambio del conjunto de caracteres. El esquema funciona para: Oracle, Sybase, MySQL y MS SQL.

Reglas del analizador

Determinadas reglas se pueden aplicar a nivel de analizador. Ejemplo de reglas del analizador son: conjuntos de caracteres definidos por el usuario, cambios en programas fuente y la emisión de veredictos de observación para la modalidad de cortafuegos. En releases anteriores, las políticas y las reglas se aplicaban al final del proceso de solicitudes en el estado de registro. En algunos casos, esto significaba un retardo en las decisiones basadas en estas reglas. Las reglas aplicadas a nivel del analizador significa que las decisiones se pueden realizar en una etapa previa.

Registro para proceso Flat

La opción de registro para proceso flat que aparece listada en la definición de política del Creador de políticas permite que el dispositivo Guardium registre información sin analizarla de forma inmediata.

Esto ahorra recursos de proceso, para que se pueda manejar un volumen de tráfico más elevado. El análisis y la fusión de esos datos en la base de datos interna de Guardium se puede realizar más tarde, ya sea en un recopilador o en una unidad de agregación.

Cuando se selecciona Registro para proceso flat (Flat Log):

- Los datos no se analizarán en tiempo real
- Los registros para el proceso flat se pueden ver en el informe de Lista de Flat Log
- El proceso fuera de línea para analizar los datos y fusionar con los dominios de acceso estándar se puede configurar a través de Gestionar > Supervisión de actividad > Proceso Flat Log.

Reglas para proceso flat

En esta sección se describen las diferencias en los usos de las reglas para el proceso Flat.

Cuando se selecciona Reglas para proceso flat:

- Las reglas a nivel de sesión se examinarán en tiempo real.
- No se evaluará ninguna regla cuando se lleve a cabo el proceso fuera de línea.

Cuando NO se selecciona Reglas para proceso flat:

- Las reglas de política se activarán en tiempo de proceso utilizando la política instalada actualmente.

Nota: Las reglas para proceso flat no funcionan con reglas de política que involucran a un campo, un objeto, un verbo SQL (mandatos), un grupo de mandatos/objetos y un grupo de campos/objetos. En el proceso Flat Log, "flat" significa que no se crea el árbol de sintaxis. Si no hay ningún árbol de sintaxis, los campos, objetos y verbos SQL no se pueden determinar.

Las siguientes acciones no funcionan con políticas de reglas para el proceso flat: LOG_FULL_DETAILS; LOG_FULL_DETAILS_PER_SESSION; LOG_FULL_DETAILS_VALUES; LOG_FULL_DETAILS_VALUES_PER_SESSION; LOG_MASKED_DETAILS.

Utilización del Seguimiento de auditoría selectivo

Utilice la opción Seguimiento de auditoría selectivo, en la sección Definición de política del Creador de políticas, para limitar la cantidad de información registrada en el dispositivo Guardium.

Esto es apropiado cuando el tráfico de interés sea un porcentaje relativamente pequeño del tráfico aceptado por los motores de inspección, o cuando todo el tráfico del que podría querer informar se puede identificar casi de forma completa.

Sin una política de seguimiento de auditoría selectivo, el dispositivo Guardium registra todo el tráfico aceptado por los motores de inspección. Cada motor de inspección en el dispositivo o en un S-TAP se configura para supervisar un protocolo de base de datos específico (por ejemplo, Oracle) en uno o varios puertos. Además, el motor de inspección se puede configurar para que acepte tráfico de subconjuntos de conexiones de cliente/servidor. Esto tiende a capturar más información que una política de seguimiento de auditoría selectivo, pero puede hacer que el dispositivo Guardium procese y almacene mucha más información de la necesaria para satisfacer sus requisitos normativos y de seguridad.

Cuando se instala una política de seguimiento de auditoría selectivo, sólo se registrará el tráfico solicitado por la política y habrá dos formas de identificar dicho tráfico:

- Especificando una serie que se puede utilizar para identificar el tráfico de interés, en el recuadro Patrón de auditoría del panel Definición de política. Permite identificar una base de datos o un grupo de tablas de base de datos, por ejemplo. Observe que un patrón de auditoría es un patrón que se aplica (a través de la coincidencia con una expresión regular) a CADA SQL que el registrador procesa para ver si coincide. Esta coincidencia de patrón es estrictamente una coincidencia de serie. NO es una coincidencia con relación a las variables de sesión (nombre de base de datos, etc) de la forma en que lo hacen las reglas de política.
- O especificando Solo auditoría o cualquiera de las acciones de registrar (Solo registrar, Registrar detalles completos, etc.) para una o más reglas de política en un panel Definición de regla. Con las reglas de política, puede ser extremadamente preciso, especificando los valores, grupos o patrones para coincidir con cualquier tipo de atributo concebible (tipo de BD, nombre de BD, nombre de usuario, etc.).

Si la política de seguridad de Guardium tiene habilitado el Seguimiento de auditoría selectivo, y se ha creado una regla en un grupo de objetos, se comprueba la serie de cada elemento del grupo. Si hay una coincidencia, se toma una decisión para registrar la información y continuar. Si la política de seguridad de Guardium tiene habilitado el Seguimiento de auditoría selectivo, y se ha creado una regla en uno de los grupos de objetos utilizando una NO designación en el grupo de objetos, todavía sigue habiendo una necesidad de comprobar la serie en cada elemento en el grupo, y decidir si registrar y continuar únicamente si ninguno de los elementos coincide. Las reglas NO designadas se comportan como reglas normales cuando se utilizan con el Seguimiento de auditoría selectivo.

Esto incluye:

- Situaciones O como, por ejemplo, reglas basadas en varios objetos o mandatos;
- Situaciones con dos condiciones NO (por ejemplo, NO parte de un grupo de objetos y NO parte de un grupo de mandatos); y,
- Situaciones con una condición NO y una condición SÍ (por ejemplo, un NO parte de un grupo de objetos y un SÍ parte de un grupo de mandatos).

Nota: Las sentencias select con sugerencias de consulta como, por ejemplo, SELECT /*+ ORDERED USE_MERGE(m) */ SELECT /*+ ORDERED */ SELECT /*+ all_rows */ etc. son procesadas por el analizador y son registradas independientemente de la definición de regla para omitirlas (al menos con la modalidad de auditoría selectiva). Esto se

debe a que una política de auditoría selectiva no debería impedir el registro de determinado SQL que podría ser necesario para otras funciones como, por ejemplo, la conversión de usuarios de aplicación.

Seguimiento de auditoría selectivo y API de sucesos de aplicación

Cuando se utiliza una política de seguimiento de auditoría selectivo, y los sucesos o los usuarios de la aplicación se están estableciendo a través de la API de sucesos de aplicación, la política debe incluir una regla de Solo auditoría que se active siempre que se encuentre un suceso de establecer/borrar aplicación o un mandato de usuario de establecer/borrar aplicación. Consulte Identificar usuarios mediante API para obtener más información sobre cómo establecer el usuario de la aplicación a través de la API de sucesos de aplicación.

Seguimiento de auditoría selectivo y Conversión de usuarios de aplicación

Cuando se utiliza una política de seguimiento de auditoría selectiva, también se está utilizando una conversión de usuarios de aplicación:

- La política ignorará todo el tráfico que no se ajuste al rol de conversión de usuarios de aplicación (por ejemplo, no desde el servidor de aplicaciones).
- Solo el SQL que coincide con el patrón para dicha política estará disponible para los informes de conversión de usuario de aplicación especiales.

Seguimiento de auditoría selectivo y especificación de un grupo vacío

Una grupo de tuplas vacías adjuntada a la regla NO originará una coincidencia de una acción de regla.

Tema principal: Políticas

Creación de políticas

Además de crear políticas, puede modificar, clonar o eliminar una política.

Creación de una política

Utilice esta sección para crear una política. Los siguientes pasos siguen los campos de menú de la pantalla Creador de políticas.

Siga estos pasos:

1. Pulse Configurar > Creador de políticas para abrir Buscador de políticas o pulse Proteger > Políticas de seguridad > Creador de políticas para abrir el Buscador de políticas.
2. Se ha creado un conjunto de políticas predefinidas (disponibles para la clonación de políticas) con reglas de extrusión, excepción y acceso para sucesos de base de datos que muestren intentos de derrotar los mecanismos de protección. Estos sucesos que generarán acciones de registro o alerta son: inicios de sesión fallidos y errores SQL desde determinados grupos o servidores, acceso a determinados objetos de base de datos por determinados usuarios o grupos, intentos de cambiar mandatos SQL GRANT entre otros más. Estas políticas predefinidas facilitan una rápida creación de políticas para el cumplimiento. Por ejemplo, GDPR, Basel II y PCI.
   Atención: Si hay disponible una versión de [plantilla] de una política predefinida, no se recomienda utilizar una versión anterior (no marcada como [plantilla]) porque no recibirá actualizaciones. En su lugar, clone la versión de la [plantilla] y personalícela según sea necesario.
3. Clone una política predefinida o pulse Nueva para abrir el panel Definición de política.
4. Especifique un nombre exclusivo para la política en el recuadro Descripción de la política. No incluya caracteres de apóstrofo en la descripción.
5. Opcional. Especifique una categoría en el recuadro Categoría. Una categoría es una etiqueta arbitraria que se puede utilizar para agrupar infracciones de política para crear informes. La categoría especificada aquí se utilizará como la categoría predeterminada para cada regla (se podrá modificar en la definición de regla).
6. Opcional. Seleccione una línea base para utilizarla en la lista de Línea base de política. Asegúrese de que la línea base seleccionada se haya generado. Si no se ha generado, el Creador de políticas no podrá sugerir reglas a partir de esa línea base. Si la línea base que desea utilizar no se visualiza en la lista, quiere decir que su ID de usuario de Guardium no ha sido asignado al rol de seguridad autorizado para utilizar dicha línea base. Póngase en contacto con el administrador de Guardium para obtener más información.

   Si la política incluye una línea base, la definición de política contendrá inicialmente solo la línea base. La acción para una línea base es siempre permitir sin continuar en la siguiente regla.

   Al añadir una línea base a una política existente, ésta se añadirá como la primera regla. Puede mover la regla de la línea base a cualquier ubicación en la política. (Tenga en cuenta que si se mueve la línea base como la última regla, no tendrá ningún efecto).

   Atención: El Creador de línea base y su funcionalidad está en desuso desde Guardium V10.1.4.
7. Opcional. Marque Registro para proceso flat para indicar que Guardium registrará datos, pero no los analizará ni agregará en la base de datos interna.
8. Si se selecciona Registro para proceso flat, opcionalmente seleccione Reglas para proceso flat para aplicar las reglas de política a los datos de Flat Log (en contraposición a los datos agregados).
9. De forma opcional, marque Seguimiento de auditoría selectivo para restringir lo que se va a registrar cuando se instale esta política:
   - Cuando se marca, sólo se registrará el tráfico solicitado por esta política. Esto es lo apropiado cuando el tráfico de interés es un porcentaje relativamente pequeño del tráfico que ven los motores de inspección. Cuando se marca, existen dos formas de indicar el tráfico que se debe registrar: mediante la especificación de una serie que se puede utilizar para identificar el tráfico de interés, en el recuadro Patrón de auditoría; o especificando Solo auditoría o cualquiera de las acciones de Registro para una o más reglas de política (las acciones de regla se describen más adelante).
   - Cuando no se marca (la situación predeterminada), el dispositivo Guardium registra todo el tráfico que ven los motores de inspección. Esto proporciona amplias funciones de seguimiento de auditoría, pero puede dar como resultado la captura y el análisis de mucha más información de la que realmente se necesita.
   - Para obtener más información, consulte el apartado Utilización del seguimiento de auditoría selectivo.
10. Pulse Guardar para guardar la definición de la política.
11. Opcionalmente, pulse Roles para asignar roles a la política.
12. Opcionalmente, pulse Comentarios para añadir comentarios a la definición.

Dónde ir desde aquí

Después de crear una nueva definición de política, utilice el panel Buscador de políticas para acceder a esa definición. Complete la definición de la política realizando una o varias de las tareas siguientes:

- Crear reglas de política manualmente. Consulte Añadir o Editar reglas.

- Si la política incluye una línea base, haga que el Creador de políticas sugiera reglas desde la línea base. Opcionalmente puede aceptar o adaptar las reglas generadas según sea necesario. Consulte la Utilización de reglas sugeridas desde la línea base.
- Haga que el Creador de políticas sugiera reglas de la lista de control de acceso (ACL) de la base de datos definida para dicha base de datos. Puede rechazar o aceptar y, opcionalmente, adaptar cada regla según sea necesario. Consulte la Utilización de reglas sugeridas desde la ACL de la base de datos.

Modificación/Clonación/Eliminación de una política

Utilice esta sección para conocer los pasos necesarios para modificar, clonar o eliminar una política.

Modificación una política

Tenga cuidado antes de modificar una definición de política: asegúrese de que entiende las implicaciones de la modificación de una política en uso. Si la política existente se tiene que volver a instalar antes de que se hayan completado todas las revisiones, es posible que la política no se instale o es posible que no se produzcan los resultados deseados cuando se instale. Por esta razón, es preferible clonar la política, de forma que la política original siempre esté disponible para volverse a instalar.

1. Pulse Configurar > Creador de políticas para abrir Buscador de políticas o pulse Proteger > Políticas de seguridad > Creador de políticas para abrir el Buscador de políticas.
2. En la lista Descripción de política, seleccione la política que se va a modificar.
3. Realice una de las siguientes acciones:
    - Para editar los valores globales de política (Categoría, opción de registro para proceso flat, etc.) pulse Modificar. Para cambiar cualquiera de estos valores, consulte Crear una política.
    - Para editar sólo las reglas, pulse Editar reglas. Para modificar los componentes de las definiciones de las reglas, consulte Adición o edición de reglas.

Clonación de una política

Hay una serie de situaciones en las que es posible que desee definir una nueva política basada en una existente, sin modificar la definición original.

1. Pulse Configurar > Creador de políticas para abrir Buscador de políticas o pulse Proteger > Políticas de seguridad > Creador de políticas para abrir el Buscador de políticas.
2. En la lista Descripción de política, seleccione la política que se va a clonar.
3. Pulse Clonar para abrir el panel Clonar política.
4. Especifique un nombre exclusivo para la nueva política en el recuadro Nombre nuevo. No incluya caracteres de apóstrofo en el nombre.
5. Para clonar las construcciones de línea base (los mandatos, básicamente) que se han generado para la línea base que se está clonando, marque el recuadro de selección Clonar construcciones.
6. Pulse Guardar para guardar la nueva política. A continuación, puede abrir y editar la nueva política a través del Buscador de políticas. Consulte Modificación de una política.

Eliminación de una política

1. Pulse Configurar > Creador de políticas para abrir Buscador de políticas o pulse Proteger > Políticas de seguridad > Creador de políticas para abrir el Buscador de políticas.
2. En la lista Descripción de política, seleccione la política que se va a clonar.
3. Pulse el botón Suprimir. Se le solicitará que confirme la acción.

Adición o edición de reglas

Utilice esta sección para añadir o editar reglas dentro de una política.

1. Pulse Configurar > Creador de políticas para abrir Buscador de políticas o pulse Proteger > Políticas de seguridad > Creador de políticas para abrir el Buscador de políticas.
2. En la lista Descripción de política, seleccione la política que se va a editar.
3. Pulse el botón Editar reglas para abrir el panel Reglas de política.
4. Realice una de las siguientes acciones:
    - Para editar una regla, pulse el botón Editar esta regla individualmente.
    - Para añadir una regla nueva, pulse uno de los botones siguientes:

      Añadir regla de acceso

      Añadir regla de excepción

      Añadir regla de extrusión (sólo estará disponible si el usuario administrador ha establecido la configuración del motor de inspección para Inspeccionar datos devueltos)

      Las coincidencias de extrusión permiten que el usuario defina el número de registros coincidentes que se agruparán conjuntamente cuando Guardium los registre e informe de los mismos. Las reglas de extrusión deben tener una acción de REGISTRAR DETALLES COMPLETOS y un nombre de regla que incluya guardium://(algún texto)?split=(número) donde (algún texto) es un texto o una de las palabras predefinidas como CREDIT CARD y (número) es el número de registros de datos devueltos por registro registrado de Guardium.
5. Los atributos que se pueden probar en cada tipo de regla varían, pero independientemente del tipo de regla, cada definición de regla empieza por los siguientes cuatro elementos:
    - Descripción de regla - Escriba un nombre descriptivo breve para la regla. Para utilizar una prueba de patrón especial, especifique el nombre de prueba de patrón especial seguido de un espacio y uno o más caracteres adicionales para hacer que el nombre de regla sea exclusivo, por ejemplo: `guardium://SSEC_NUMBER employee`.
    - Categoría - La categoría se registrará con infracciones. Se utiliza con fines de agrupación y creación de informes. Si no se especifica nada, se utiliza el valor predeterminado para la política.
    - Clasificación - Especifique opcionalmente una clasificación en el recuadro Clasificación. Al igual que con la categoría, éstas se registran con excepciones y se pueden utilizar con fines de agrupación y creación de informes.
    - Gravedad - Seleccione un código de gravedad: Información, Bajo, Medio o Alto (el valor predeterminado es Info).
6. Utilice los campos restantes del panel Definición de regla para especificar cómo se realizará la coincidencia de la regla. La mayoría de los campos están disponibles para las reglas de acceso, excepción y extrusión. Algunos campos sólo están disponibles después de seleccionar otras opciones. Para obtener una referencia de

todos los campos disponibles en los paneles de definición de reglas, consulte Referencia de definición de regla. Asimismo, para obtener instrucciones sobre cómo utilizar combinaciones de grupos y valores individuales, consulte Especificación de valores y/o grupos de valores en reglas.

7. Para cada tipo de regla, se puede especificar una o varias expresiones regulares en un recuadro de Patrón, para la coincidencia con relación a series en el tráfico. Especifique la expresión de forma manual, o pulse el icono RE para abrir la herramienta Crear expresión regular, que permite especificar y probar expresiones regulares.
8. Sólo en el caso de las reglas de excepción, en el recuadro Tipo de excepción seleccione un único tipo de excepción al que la regla será sensible. El recuento de la regla sólo se incrementará cuando se encuentre el tipo de excepción seleccionado.
9. Cuando se selecciona una acción de regla, se habilitan los dos campos siguientes:
    - Rec. mín. - Especifique el número mínimo de veces que se debe producir la coincidencia de la regla antes de que se desencadene la acción de regla. El recuento de veces que se ha cumplido la regla se restablecerá cada vez que se desencadena la acción o cuando caduque el intervalo de restablecimiento. El valor predeterminado de cero es idéntico a 1, lo que significa que cada vez que se cumpla la regla se desencadenará la acción.
    - Intervalo de restablecimiento (minutos) - Sólo se utiliza cuando el recuento mínimo es mayor que cero y, en ese caso, es necesario. Especifique el número de minutos después de los cuales el contador de reglas se restablecerá a cero. El contador también se restablece a cero cada vez que se desencadena la acción de la regla.
10. Seleccione el recuadro Continuar en la siguiente regla para indicar que cuando se satisface esta regla y se desencadena su acción, la prueba de la misma solicitud, excepción o resultados debería continuar en la regla siguiente. Esto significa que se pueden satisfacer varias reglas y se pueden tomar varias acciones basándose en una única solicitud o excepción. Si no se marca (el valor predeterminado), no se comprobará ninguna regla adicional cuando se satisfaga esta regla. Si se marca, la prueba de las reglas continuará con la siguiente regla, independientemente de si se satisface o no esta regla.
11. Cuando se marca el recuadro Val. Grab., la construcción real que hace que se satisfaga la regla se registrará en el atributo de serie SQL y estará disponible en los informes. Si no se marca, no se registrará ninguna sentencia SQL.
12. Las plantillas de mensaje se utilizan para generar alertas. Se crean y modifican varias plantillas de mensajes con nombre desde el perfil global.
13. Seleccione la acción a realizar cuando se satisfaga la regla.
14. Si se especifica una acción de alerta, se abre el panel Notificación y como mínimo se debe definir un tipo de notificación. Para obtener instrucciones sobre cómo añadir notificaciones, consulte Notificaciones.
15. Pulse Guardar para guardar la regla. Esta acción cierra el panel de Definición de regla y se vuelve al panel de Reglas de política.

Filtración de reglas para visualizar solo un subconjunto

Cuando una política contiene muchas reglas, puede ser útil ver un subconjunto de las reglas que tienen atributos comunes.

El recuadro Filtro del panel Definición de reglas se puede utilizar para este propósito. El proceso de definición de un filtro es similar al proceso de definición de una regla.

1. Pulse Configurar > Creador de políticas para abrir Buscador de políticas o pulse Proteger > Políticas de seguridad > Creador de políticas para abrir el Buscador de políticas.
2. En la lista Descripción de política, seleccione la política que se va a visualizar o modificar.
3. Pulse Editar reglas.
4. En el recuadro de Filtro, realice una de las acciones siguientes:
    - Seleccione un filtro desde la lista de Filtro.
    - Pulse Editar para modificar una definición de filtro.
    - Pulse Nuevo para definir un filtro nuevo.

    Una vez se visualice el conjunto de reglas filtrado, puede realizar cualquiera de las acciones descritas en esta sección en las reglas visualizadas.

Copia de reglas

Utilice este procedimiento para copiar reglas seleccionadas de una política a otra, o a una ubicación distinta en la misma política.

Todas las reglas copiadas se copiarán en una única ubicación - después de la regla 3, por ejemplo. Para copiar reglas en distintas ubicaciones en la política de recepción, realice varias operaciones de copia o copie todas las reglas en una sola operación y, a continuación, edite la política de recepción para mover las reglas según sea necesario.

1. Pulse Configurar > Creador de políticas para abrir Buscador de políticas o pulse Proteger > Políticas de seguridad > Creador de políticas para abrir el Buscador de políticas.
2. En la lista Descripción de política, seleccione la política desde la que desea copiar una o más reglas.
3. Pulse Editar reglas.
4. Marque el recuadro de selección de cada regla que se va a copiar.
5. Pulse Copiar reglas.
6. Desde Copiar las reglas seleccionadas en la política, seleccione la política que va a recibir las reglas copiadas.
7. En la lista Insertar después de regla, seleccione la regla después de la cual se deben insertar las reglas copiadas o seleccione Superior para insertar las reglas copiadas al principio de la lista.
8. Pulse Copiar. Se le informará sobre el éxito de la operación.
9. Ahora debería editar la política en la que ha copiado las reglas, para verificar que ha copiado las reglas correctas en la ubicación correcta.

Utilización de reglas sugeridas desde la línea base

Utilice el Creador de políticas para sugerir reglas desde la línea base que se incluye en la política.

1. Pulse Configurar > Creador de políticas para abrir Buscador de políticas o pulse Proteger > Políticas de seguridad > Creador de políticas para abrir el Buscador de políticas.
2. En la lista Descripción de política, seleccione la política con la que desea trabajar. (Debe incluir una línea base).
3. Pulse el botón Editar reglas.
4. Establezca el valor de recuento mínimo de reglas. Es el número mínimo de mandatos like que el sistema debería encontrar con el propósito de sugerir una regla. El valor predeterminado es de cero. Cuanto más pequeño sea el número especificado, más reglas sugeridas generará el sistema. (Tenga en cuenta que el recuento que se visualiza en el panel de reglas sugeridas no refleja este valor).
5. Establezca el valor de recuento mínimo de grupos de objetos, para determinar el número de instancias de un grupo de objetos que el sistema debe encontrar para generar un grupo de objetos sugeridos. El valor predeterminado es uno. Cuanto más pequeño sea el número que especifique aquí, mayor será el número de grupos sugeridos.
6. Pulse el botón Sugerir reglas. Las reglas sugeridas se visualizan en una ventana aparte, en el panel Reglas sugeridas.
7. Las reglas sugeridas se clasifican en orden descendente según el número de apariciones en el periodo de la línea base, que aparece listado para cada regla sugerida. Si selecciona una o varias de las reglas sugeridas y pulsa Guardar, éstas se insertarán en el mismo orden, justo antes de la regla BASELINE en el panel de Reglas de política. A continuación, puede cambiar el orden de las reglas sugeridas o editarlas según sea necesario, desde el panel Reglas de política.

8. Expanda las reglas y compruebe la pertenencia de los grupos de objetos sugeridos. En la columna Objeto del panel de Reglas sugeridas, si se ha creado alguno de los grupos de objetos sugeridos, estos empiezan con el nombre de Grupo de objetos sugerido y se visualizan como enlaces de hipertexto. Para obtener información acerca de cómo ver, aceptar o rechazar grupos de objetos sugeridos, consulte Utilización de grupos de objetos sugeridos.
9. Marque el recuadro Seleccionar para cada regla sugerida para incluirla en la política.
10. Pulse Guardar para aceptar las reglas seleccionadas.
11. Ahora podrá editar o modificar las reglas sugeridas como lo haría con cualquier regla que hubiese añadido de forma manual.

Utilización de grupos de objetos sugeridos

El Creador de políticas puede sugerir reglas tanto desde la línea base incluida en la política como de la política de seguridad de la base de datos (interna para el DBMS) definida para un servidor.

En ambos casos, intenta generar el conjunto mínimo de reglas agrupando objetos (tablas, procedimientos o vistas) de base de datos en grupos de objetos sugeridos. Puede aceptar o rechazar los grupos de objetos sugeridos.

Antes de aceptar un grupo de objetos sugeridos, puede editar el campo generado Descripción de grupo (por ejemplo, Suggested Object Group603-25 11:54) para proporcionar un nombre más significativo. Después de aceptar un grupo de objetos sugeridos, puede ver su pertenencia. Puede rechazar el uso de ese grupo dentro de cualquier regla sugerida, pero no puede editar la pertenencia de dicho grupo.

Si rechaza un grupo de objetos sugeridos, la regla sugerida para ese grupo se sustituye por una regla sugerida aparte para cada miembro del grupo rechazado. Puede aceptar o rechazar cada una de las reglas sugeridas por separado. Después de aceptar una regla sugerida, puede editar esa regla.

Utilización de grupos de objetos sugeridos

Los grupos de objetos sugeridos se muestran en la columna Objeto del panel Reglas sugeridas como enlaces de hipertexto que empiezan por las palabras Grupos de objetos sugeridos.

Para ver la pertenencia a un grupo de objetos sugeridos, pulse en el enlace de hipertexto de dicho grupo. Si el grupo todavía no se ha aceptado, la pertenencia del grupo se visualiza en el panel Editar grupo. Si el grupo ya se ha aceptado, se visualiza en el panel Ver grupo.

Aceptación de grupos de objetos sugeridos

Para aceptar un grupo de objetos sugeridos:

1. Especifique un nombre significativo en el campo Descripción de grupo en el panel Editar grupo. (No es necesario, pero se recomienda encarecidamente). No incluya caracteres de apóstrofo en el nombre. Esta es la única oportunidad que tiene que denominar a este grupo. De lo contrario, el grupo obtiene un nombre que empieza por Grupo de objetos sugeridos seguido de un número, tal como se ha descrito anteriormente.
2. Pulse Guardar para aceptar el grupo editado para la regla sugerida o pulse Guardar para todas para aceptar el grupo editado para todas las reglas sugeridas en las que aparece. El nuevo nombre de objeto sustituirá al antiguo en la regla.

Rechazo de grupos de objetos sugeridos

Cuando se rechaza un grupo de objetos sugeridos, el uso de dicho grupo se sustituye por una o más reglas sugeridas. Para rechazar un grupo de objetos sugeridos, realice una de las acciones siguientes:

- Para rechazar el grupo sólo para esta regla sugerida: Pulse el botón Rechazar.
- Para rechazar el grupo para todas las reglas sugeridas: pulse el botón Rechazar para todas.

Nota: Si acepta un grupo de objetos sugeridos en una regla, abra ese mismo grupo de objetos sugeridos de nuevo desde otra regla y, a continuación, pulsa el botón Rechazar para todas, ese grupo se conservará en cualquier regla en la que se haya aceptado explícitamente y se rechazará en las reglas restantes en las que se ha utilizado.

Utilización de reglas sugeridas desde la ACL de la base de datos

Para un servidor de bases de datos especificado, el Creador de políticas puede sugerir reglas de acceso utilizando la política de seguridad definida internamente por el DBMS.

El Creador de políticas hace esto examinando los permisos otorgados a los grupos de usuarios y a los objetos de base de datos (tablas, procedimientos y vistas) dentro del DBMS y, a continuación, agrupando los objetos de base de datos en grupos de objetos sugeridos para que el número total de reglas sugeridas se pueda minimizar. Puede aceptar o rechazar cualquier grupo de objetos sugerido (consulte Utilización de grupos de objetos sugeridos). También puede aceptar o rechazar cualquier regla sugerida.

Para hacer que el Creador de políticas sugiera reglas de la ACL de la base de datos:

Nota: Al sugerir reglas de la ACL de la base de datos, el sistema no utiliza los campos Recuento mínimo de reglas ni Recuento mínimo de grupos de objetos. Estos campos sólo se utilizan cuando se sugieren reglas desde la línea base.

1. Pulse Sugerir desde BD para abrir el panel Definición de base de datos en una ventana aparte del navegador.
2. Pulse Añadir origen de datos para seleccionar la base de datos desde la que desea acceder a la ACL de la base de datos.
   Nota: Si se añade un origen de datos de Oracle, DB2 o DB2 for z/OS para acceder a la ACL de la base de datos, se inhabilitará la sección Parámetros de consulta en la ventana emergente de Definición de base de datos.
3. Pulse Sugerir reglas para generar las reglas. El panel de Reglas sugeridas se abre en una ventana aparte (tal como se ha descrito anteriormente, para las Reglas sugeridas desde la línea base). Si selecciona una o varias de las reglas sugeridas y pulsa Guardar, éstas se insertarán en el mismo orden en la lista de reglas en el panel de Reglas de política, justo antes de la regla BASELINE. Si no hay una regla BASELINE, se insertarán al principio de la lista. Una vez que se hayan insertado las reglas sugeridas en el panel Reglas de política, puede cambiar el orden de las reglas o editarlas, según sea necesario.
4. Compruebe la pertenencia de los grupos de objetos sugeridos. En la columna Objeto, todos los grupos de objetos sugeridos que se han creado empiezan con el nombre de Grupo de objetos sugeridos y se visualizan como enlaces de hipertexto (en azul y subrayado). Para obtener información sobre cómo ver, editar, aceptar o rechazar grupos de objetos sugeridos, consulte Utilización de grupos de objetos sugeridos).
5. Marque el recuadro Seleccionar para cada regla sugerida para incluirla en la política. Pulse Guardar para aceptar las reglas seleccionadas.

Utilización del Simulador de políticas

Utilice el Simulador de políticas para probar las reglas de acceso sin instalar la política.

No permite probar las reglas de excepción ni las reglas de extrusión. El simulador reproduce el tráfico de red registrado y aplica todas las reglas de acceso de la política. Genera un informe especial en una ventana aparte, listando el SQL que desencadenó alertas o acciones de solo registrar. Este informe incluye las siguientes columnas:

Indicación de fecha y hora, Nombre de categoría, Descripción de regla de acceso, IP de cliente, IP de servidor, Nombre usuario de BD, Serie SQL completo, Descripción de la gravedad y Recuento de infracciones de reglas de política. Utilice el mandato de CLI, store allow_simulation, para activar el botón de Simulación de política en la interfaz gráfica de usuario.

El Simulador de políticas solo de puede utilizar probar sólo los siguientes tipos de acciones de regla de acceso:

- Solo registrar
- Cualquier acción de alerta: Alertar diariamente, Alertar una vez por sesión, Alertar por coincidencia, Alerta por granularidad de tiempo

El Simulador de políticas no generará ningún resultado si la política incluye acciones de registro distintas de Sólo registrar. Para utilizar el simulador para este tipo de política, cambie temporalmente todas las acciones de registro a Solo registrar.

Para utilizar el Simulador de políticas:

1. Pulse Configurar > Creador de políticas para abrir Buscador de políticas o pulse Proteger > Políticas de seguridad > Creador de políticas para abrir el Buscador de políticas.
2. En la lista Descripción de política, seleccione la política con la que desea trabajar.
3. Pulse Editar reglas.
4. Pulse el botón Simulador de políticas para abrir el panel Simulador de políticas.
5. Proporcione las fechas Desde y Hasta para definir el periodo de tiempo que se debe utilizar para la simulación.
   Nota: Los datos históricos se pueden archivar y depurar desde el dispositivo Guardium en una planificación definida por el administrador de Guardium. Asegúrese de que los datos del periodo de tiempo que especifique estén disponibles (y no se hayan depurado).
6. Pulse Probar. Cuando se inicia la prueba y mientras se está ejecutando, se visualiza el mensaje * está en ejecución en el panel del Simulador de políticas. Cuando se completa la prueba, se abre un informe especial en una ventana aparte que lista todas las coincidencias de reglas que se han registrado. Si no se han desencadenado reglas de solo registrar o alertas, recibirá un mensaje `No hay disponible informe de profundizar`. En este último caso, es posible que no haya incluido suficientes datos en el periodo de prueba.

Tema principal: Políticas
Información relacionada:
Creación e instalación de una política (vídeo)
Grupos y políticas de Guardium (vídeo)

Instalación de políticas

Utilice este tema para instalar políticas en el recopilador de Guardium y para modificar la planificación.

Soporte a varias políticas

1. Pulse Configuración > Creador de políticas para abrir el Buscador de políticas o pulse Proteger > Políticas de seguridad > Instalación de políticas para abrir el Instalador de políticas.
2. Seleccione la política que se va a instalar en el recuadro Descripción de política.
3. Realice una de las siguientes acciones:
   - Pulse Instalar para instalar la política de forma inmediata.
   - Pulse Modificar planificación para abrir el programa de utilidad de planificación de propósito general, para planificar la instalación de la política.

Visualización de reglas de política para la política instalada

Se permite instalar más de una política al mismo tiempo. Todas las políticas instaladas están disponibles para realizar sus acciones. Existen dos limitaciones: las políticas definidas como políticas de auditoría selectiva no se pueden combinar con políticas no definidas como políticas de auditoría selectiva, y las políticas definidas como de Flat Log no se pueden combinar con políticas que no definidas como de Flat Log. Si se intentan combinar políticas, se generará un mensaje de error al instalar estas políticas de tipos distintos.

El orden de aparición se puede controlar durante la instalación de la política como, por ejemplo, colocándolas al principio, al final o en algún lugar intermedio. Sin embargo, el orden de aparición no se puede editar con posterioridad.

También hay un botón de Desinstalar política para eliminar una política instalada con anterioridad.

La primera política instalada tiene un significado especial, ya que establece el valor de los parámetros de política global. Estos parámetros son: Patrón global; Es una auditoría selectiva; Máscara de red de servidor y cliente; Cliente codificado e ID de grupo de servidores.

Este soporte para varias políticas está disponible a través de la interfaz gráfica de usuario (Configuración > Herramientas y vistas > Instalación de políticas) y a través de GuardAPI.

Visualización de reglas de política para la política instalada

Desde el panel de Políticas instaladas actualmente, cualquier usuario puede ver las reglas de la política instalada y, además, los usuarios autorizados podrán abrir la política para editarla.

1. Pulse Configuración > Creador de políticas para abrir el Buscador de políticas o pulse Proteger > Políticas de seguridad > Instalación de políticas para abrir el Instalador de políticas.
2. Pulse el enlace Política instalada para visualizar las reglas de política. Los usuarios autorizados tendrán un botón adicional habilitado: Para abrir la política para su edición en el Creador de políticas, pulse el botón Editar política instalada.

Planificador de dependencias de trabajo

El recopilador de Guardium tiene muchas tareas que se pueden planificar para su ejecución de forma periódica como, por ejemplo, Instalación de políticas, Procesos de auditoría o Actualizaciones de grupo entre otros. La característica de Dependencias de trabajo encuentra todos los trabajos que tienen una relación directa y un impacto en el éxito de la ejecución de la tarea que está intentando planificar. Si no encuentra los trabajos definidos como requisitos previos para el trabajo que está intentando planificar, existe la posibilidad de que la tarea se base en datos inexactos, lo que puede conducir a resultados falsos o inexactos.

Puntos destacados de la característica

- El usuario marca un trabajo planificado para buscar y ejecutar sus dependencias en tiempo de ejecución.
- Cuando el planificador ejecuta el trabajo, de forma automática encuentra todos los trabajos subordinados y los ejecuta ordenadamente.
- Existe una secuencia de intento en el caso de que se produzca una anomalía.

Dependencias

- Identifica escenarios que precisan dependencias.
- Identifica trabajos ejecutables frente a trabajos no ejecutables.
- Calcula dependencias de trabajos definidos de forma previa.

Trabajo	Trabajo de requisito previo sugerido	Razón
Instalación de políticas	Grupos que están definidos en alguna de las políticas (a ser instaladas) y que están planificadas o no planificadas para ser cumplimentadas por el mecanismo de Cumplimentar desde consulta.	Las reglas de política que utilizan grupos deben tener sus datos de grupo actualizados antes de ser instaladas.
Instalación de políticas	Procesos de auditoría que incluyen una tarea de Clasificación de auditoría, donde la tarea de clasificación tiene una acción de Añadir a grupo de objetos, Añadir a grupo de objetos/campos o Añadir a regla de acceso.	Las reglas de política que utilizan grupos deben tener sus datos de grupo actualizados antes de ser instaladas.
Proceso de auditoría	Trabajos de subida de tabla personalizada donde se hace referencia al nombre de tabla personalizada (en la cláusula "from") por parte de una tarea de auditoría de tipo Informe.	Los datos de las tablas personalizadas a los que hace referencia una tarea de auditoría de tipo Informe se deben cumplimentar con datos actualizados antes de que se planifique la ejecución del proceso de auditoría.
Proceso de auditoría	Grupos definidos en una condición de una tarea de auditoría de tipo Informe que estén planificadas o no planificadas para ser cumplimentadas por el mecanismo de Cumplimentar desde consulta.	Los grupos a los que hace referencia la condición de la consulta se deben cumplimentar con datos actualizados antes que se ejecute una tarea de auditoría del tipo Informe.
Cumplimentar desde consulta	Tablas de subida personalizadas con entidades de la consulta que se utiliza para cumplimentar un grupo.	
Proceso de auditoría	Importar	Solo significativo para un agregador. Este requisito previo garantiza que la información se importa desde todas las unidades agregadas antes de que se pueda ejecutar cualquier proceso de auditoría.

Mejoras en el planificador

- Encontrar dependencias de trabajo cuando se ejecuta un trabajo planificado.
- Ejecutar dependencias de trabajo en orden.

Los trabajos ejecutables se pueden planificar, no así los trabajos no ejecutables.

Un grupo es un trabajo que no ejecutable.

Cumplimentar desde consulta en un grupo es ejecutable.

Las dependencias directas son objetos que están vinculados de forma conjunta por su definición, por ejemplo, una política que depende de una regla y una regla que depende de unos grupos.

Las dependencias indirectas son objetos que se vinculan de forma lógica, por ejemplo, la ejecución de procesos de auditoría antes de la instalación de políticas.

Soporte de interfaz gráfica de usuario

1. Opción de recuadro de selección, Ejecutar automáticamente trabajos dependientes, después de seleccionar Crear planificación desde Instalación de políticas.
2. Pulse Guardar para planificar el proceso. Esto notifica al usuario el estado de las dependencias.

Soporte de GuardAPI

Mandatos de dependencia de trabajo de GuardAPI:

CLI> grdapi add_job_dependency

Parámetros de función:

dependOnJobExecutedWithin - Serie

dependOnTrigger - Serie - obligatorio

intervalBetweenRetries - Entero

jobRetries - Entero

jobTrigger - Serie - obligatorio

runIfDependOnJobReturns - Serie

api_target_host - Serie

Utilice este mandato GuardAPI para la ejecución automática de dependencias:

> grdapi auto_execute_suggested_dependencies jobTrigger=*<nombre desencadenante de trabajo planificado>*

CLI> grdapi auto_execute_suggested_dependencies

Parámetros de función:

jobTrigger - Serie - obligatorio

api_target_host - Serie

CLI> grdapi delete_job_dependencies

Parámetros de función:

dependOnTrigger - Serie

jobTrigger - Serie - obligatorio

api_target_host - Serie

CLI> grdapi disable_auto_execute_suggested_dependencies

Parámetros de función:

jobTrigger - Serie - obligatorio

api_target_host - Serie

CLI> grdapi list_job_dependencies_tree

Parámetros de función:

jobTrigger - Serie - obligatorio

api_target_host - Serie

Para obtener una lista de todos los desencadenantes/trabajos planificados, ejecute el mandato GuardAPI:

> grdapi list_scheduler_jobs

CLI> grdapi list_suggested_job_dependencies

Parámetros de función:

jobTrigger - Serie - obligatorio

api_target_host - Serie

CLI> grdapi list_existing_job_dependencies

Parámetros de función:

jobTrigger - Serie - obligatorio

api_target_host - Serie

CLI> grdapi modify_job_dependency

Parámetros de función:

dependOnJobExecutedWithin - Serie

dependOnTrigger - Serie - obligatorio

intervalBetweenRetries - Entero

jobRetries - Entero

jobTrigger - Serie - obligatorio

runIfDependOnJobReturns - Serie

api_target_host - Serie

CLI> grdapi show_job_dependency_execution_profile

Parámetros de función:

dependOnTrigger - Serie - obligatorio

jobTrigger - Serie - obligatorio

api_target_host - Serie

Ejecución del planificador

El planificador comprobará si hay dependencias de trabajo cuando sea el momento de ejecutar un trabajo.

Las dependencias se ejecutan en orden inverso.

Ejemplo: Dado un árbol de dependencias:

Instalación de

política (Ejecutable)						
	Proceso de auditoría (Ejecutable / Dependencia indirecta)					
		Tarea de auditoría				
			Proceso de clasificación			
				Política de clasificación		
					Acción de política de clasificación	
						Grupo (Ejecutable/directa - Cumplimentar desde consulta)

El orden de ejecución será: Cumplimentar grupo desde consulta → Proceso de auditoría → Instalación de políticas

El planificador ejecutará cada una de las dependencias y esperará a que finalice.

La ejecución de un árbol de dependencias completo puede tardar bastante tiempo en completarse, pero garantizará que todas las dependencias se ejecuten en el orden correcto.

Manejo de errores

Si alguna falla alguna de las dependencias, el trabajo actualmente planificado por el planificador no se ejecutará.

Si se produce un fallo, se escribe un mensaje de error en el informe de Excepción de trabajos planificados.

Existe la posibilidad de establecer el número de reintentos del trabajo dependiente en trabajos anteriores. El valor predeterminado es 3. Un valor válido tiene que ser ≥ 0. Se puede establecer, en minutos, el intervalo entre reintentos. El valor predeterminado es 3. Un valor válido tiene que ser ≥ 0.

Tema principal: Políticas

Campos de definición de regla

Puede utilizar estos campos al definir reglas de política.

Tabla 1. Tabla de referencia de campos de definición de regla

Campo	Descripción
Acción	Indica la acción que debe realizarse cuando la regla es verdadera. Para obtener una descripción completa de todas las acciones de regla, consulte Visión general de acciones de regla.
Existe suceso de aplicación	Coincidencia de solo suceso de aplicación. Consulte Nota de suceso de aplicación.
Valores de suceso de aplicación	Coincidencia de los valores de Fecha, Numérico y Texto de suceso de aplicación. También permite como opción elegir un Grupo de la serie del suceso. Consulte Nota de suceso de aplicación.
Tipo de suceso (Aplicación)	Coincidencia con el suceso de aplicación especificado. Consulte Nota de suceso de aplicación.
Nombre de usuario de suceso (Aplicación)	Coincidencia de solo el nombre de usuario de suceso de aplicación especificado. Consulte Nota de suceso de aplicación.
Nota de suceso de aplicación	No se pueden utilizar los campos Suceso de aplicación cuando se marca el recuadro Flat Log.
Usuario aplic.	Usuario de aplicación. Consulte Especificación de valores y/o grupos de valores en reglas.
Categoría	Etiqueta arbitraria que se puede utilizar para agrupar infracciones de política a efectos de crear informes. Se puede especificar una categoría predeterminada en la definición de la política, no obstante, el valor predeterminado se puede modificar para cada regla.
Clasificación	Etiqueta arbitraria que se puede utilizar para agrupar infracciones de política a efectos de crear informes. Se puede especificar una clasificación predeterminada en la definición de la política, no obstante, el valor predeterminado se puede modificar para cada regla.
Información de cliente	Información de cliente de DB2: Solo para reglas de acceso. Solo para z/OS, un campo CLIENT INFO (y CLIENT_INFO_GROUP_ID) será visible si el DB_TYPE es DB2, Perfil DB2 COLLECTION o Perfil VSAM COLLECTION. El tipo de información que se puede colocar en este campo es USER=x; WKSTN=y; APPL=z.

Campo	Descripción
IP de cliente	Deseleccione el recuadro No para incluir, o marque el recuadro No para excluir: • Cualquier cliente: Deje todos los campos de cliente en blanco. El recuento se incrementará cada vez que un cliente satisfaga la regla. (No puede dejar todos los campos en blanco si el recuadro No está marcado). • Todos los clientes seleccionados por una dirección y máscara IP: Especifique una dirección IP de cliente en el primer recuadro y la máscara de red en el segundo recuadro. El recuento se incrementará cada vez que uno de los clientes especificados satisfaga la regla. Por ejemplo, para seleccionar todos los clientes en la subred 192.168.9.x, especifique 192.168.9.1 en el primer recuadro 255.255.255.0 en el segundo recuadro. Para obtener más información sobre la selección de direcciones IP, consulte Selección de direcciones IP utilizando una máscara. • Un grupo de clientes: Seleccione un grupo de direcciones IP de cliente en la lista desplegable de Grupo o pulse el botón Grupos para definir un grupo nuevo y, a continuación, seleccionar dicho grupo. El recuento se incrementará cada vez que un miembro del grupo seleccionado satisfaga la regla. • Todos los clientes seleccionados por una dirección y máscara IP Y un grupo de clientes: Utilice los campos IP de cliente y Grupo. El recuento se incrementará cada vez que un cliente especificado utilizando cualquiera de los dos métodos satisfaga la regla. Comodines permitidos en la dirección de IP. El comodín % está permitido en una política para un grupo de IP de cliente.
IP de cliente/Programa fuente/Usuario de BD/IP de servidor/Nombre de servicio	Grupo de tuplas de 7 elementos: IP cliente/Aplic fuente/Usuario BD/IP servidor/Nombre servicio/Usuario SO/BD Grupo de tuplas de 5 elementos disponible para las reglas de acceso, excepción y extrusión. Una tupla combina varios atributos de forma conjunta para formar un miembro de grupo individual. La tupla da soporte al uso de una barra y un carácter comodín (%). No da soporte al uso de una doble barra invertida. El comodín % está permitido en una política para un grupo de IP de cliente/Programa fuente/Usuario BD/IP de servidor/Nombre de servicio.
MAC cliente	Para hacer que la regla sea sensible a una dirección MAC de cliente individual, especifique la dirección en el formato nn:nn:nn:nn:nn:nn, donde cada n es un dígito hexadecimal (0-F) o especifique un punto (.) en el recuadro MAC cliente para indicar que se debe mantener un recuento separado para cada dirección MAC cliente o deje el recuadro MAC cliente vacío para ignorar las direcciones MAC de cliente.
Mandato	El mandato. Consulte Especificación de valores y/o grupos de valores en reglas si un grupo de mandatos no se puede editar, y la etiqueta y/o grupo cambia a Sólo recopilar, lo que indica que sólo deben seleccionarse los mandatos de los grupos seleccionados. Si se selecciona el recuadro Todo, cada campo de la sentencia SQL debe ser un miembro del grupo.
Continuar en la siguiente regla	Si se marca, la prueba de las reglas continuará con la siguiente regla, independientemente de si se satisface o no esta regla. Esto significa que pueden satisfacerse varias reglas (y realizar varias acciones) mediante una única excepción o sentencia SQL. Si no se marca (el valor predeterminado), no se comprobará ninguna regla adicional para la transacción actual cuando se satisfaga esta regla.
Patrón de datos	Cada tipo de regla (Acceso, Excepción, Extrusión) puede tener un patrón de datos. Es necesario para las reglas de extrusión. Para utilizar en la definición de reglas de extrusión - Una expresión regular que debe coincidir, en el recuadro del Patrón de datos. Pulse el botón Expresión regular para abrir la herramienta Crear expresión regular, que permite especificar y probar expresiones regulares. Esto permite patrones de enmascaramiento más complejos. Coloque los paréntesis alrededor de la sección que se debe enmascarar. Utilice esta función para enmascarar los datos recuperados de la base de datos. Por ejemplo, Windows S-TAP: ([0-9][0-9][0-9][0-9[-,]?[0-9][0-9][0-9][0-9][-,]?[0-9][0-9][0-9][0-9][-,]?)[0-9][0-9][0-9][0-9] Unix S-TAP: ([0-9]{4}[-,]?[0-9]{4}[-,]?[0-9]{4}[-,]?)[0-9]{4}[ ]{0,20} Expresiones regulares adicionales (Regex) para su uso solamente en patrones de datos con una acción de Redactar (Limpiar): Para Windows S-TAP Nombre: Patrón: Enmascarado como: SCRUB_SSN_ANSI AAA-AA-AAAA ***-***-AAAA SCRUB_SSN_UNICODE UUU-UU-UUUU ***-***-UUUU SCRUB_CC_SPACES_ANSI AAAA AAAA AAAA AAAA **** **** **** AAAA SCRUB_CC_SPACES_UNICODE UUUU UUUU UUUU UUUU **** **** **** UUUU SCRUB_CC_SOLID_ANSI AAAAAAAAAAAAAAAA ************AAAA SCRUB_CC_SOLID_UNICODE UUUUUUUUUUUUUUUU ************UUUU SCRUB_CC_AX_SOLID_ANSI AAAAAAAAAAAAAAA ***********AAAA SCRUB_CC_AX_SOLID_UNICODE UUUUUUUUUUUUUUU ***********UUUU UNIX S-TAP Nombre: Patrón: Enmascarado como: SCRUB_SSN_ANSI AAA-AA-AAAA ***-***-AAAA SCRUB_SSN_UNICODE UUU-UU-UUUU ***-***-UUUU SCRUB_CC_SPACES_ANSI AAAA AAAA AAAA AAAA A*** **** **** 1234 SCRUB_CC_SPACES_UNICODE UUUU UUUU UUUU UUUU U*** **** **** **** SCRUB_CC_SOLID_ANSI AAAAAAAAAAAAAAAA A*************** SCRUB_CC_SOLID_UNICODE UUUUUUUUUUUUUUUU U*************** SCRUB_AMEX_SOLID_ANSI AAAAAAAAAAAAAAAA A*************** SCRUB_AMEX_SOLID_UNICODE UUUUUUUUUUUUUUUU U***************

Campo	Descripción
	Expresión regular con Redactar - Las expresiones regulares (regex) en la solución IBM Security Guardium (que incluye el enmascaramiento en la política) se ejecutan en el dispositivo, y permiten funcionalidades de expresiones regulares avanzadas. Sin embargo, la biblioteca de expresiones regulares para su uso con la redacción se ejecuta en el kernel del servidor de bases de datos y está limitada a las expresiones regulares más básicas. Con la redacción solo se pueden utilizar los patrones de expresiones regulares básicos. Por ejemplo, no es posible utilizar la nomenclatura de expresión regular [0-9]* para indicar cualquier número de dígitos. Es necesario utilizar la nomenclatura de expresión regular básica [0-9]-[0-9]-[0-9]... para especificar una secuencia de dígitos. Nota: S-TAP sólo aceptará los nombres de patrón SCRUB predefinidos; ignorando cualquier otro nombre. Regla de acceso, patrón de datos y carácter de reemplazamiento - La utilización de un patrón de datos, por ejemplo, [a-z,2}{3}([_][0-9]{1,2}) con un carácter de reemplazamiento * cambiará los valores entre paréntesis en el patrón de datos a ***. Utilice esta función para enmascarar valores. Conjuntos de caracteres definidos por el usuario Disponibles para Oracle, Sybase, MySQL, MSSQL y para reglas de extrusión únicamente, los usuarios tienen la posibilidad de influir en el conjunto de caracteres utilizado mediante la definición de reglas de extrusión especiales. Estas reglas de política de conjunto de caracteres únicamente se utilizan para establecer el conjunto de caracteres en el que el usuario desea convertir el tráfico, establecer una acción es irrelevante. Para poder tener una acción para ese tráfico, el usuario necesita definir reglas adicionales después de la regla del conjunto de caracteres. Son posibles dos ejemplos para establecer una regla de conjunto de caracteres (hint o force) tal como se define en los siguientes ejemplos: Ejemplo de regla de extrusión (con hint) Convertirá el tráfico por conjunto de caracteres tal como esté definido en la regla de extrusión de la política instalada SOLO si la conversión normal falla. Conjunto de caracteres EUC-JP (código 274). Patrón de regla de extrusión: guardium://char_set?hint=274 Ejemplo de regla de extrusión (con force) Convertirá el tráfico por conjunto de caracteres tal como esté definido en la regla de extrusión de la política instalada para TODOS los datos. Conjunto de caracteres EUC-JP (código 274). Patrón de regla de extrusión: guardium://char_set?force=274 Consulte Lista de códigos de conjuntos de caracteres posibles al final de este tema. Nota: Tenga en cuenta que las reglas de extrusión habitualmente se adjuntan a la sesión con retraso. Por lo tanto, en sesiones cortas o al principio de una sesión es posible que el cambio del conjunto de caracteres no sea inmediato.
Nombre de BD	Nombre de la base de datos. Consulte Especificación de valores y/o grupos de valores en reglas.
Tipo de BD	Tipos de BD soportados Para reglas de acceso: Cassandra, CIFS, CouchDB, DB2, DB2 COLLECTION PROFILE* (solo para utilizar con z/OS), FTP, GreenPlumDB, Hadoop, HTTP, IBM® INFORMIX (DRDA), IBM iSeries, IMS, IMS COLLECTION PROFILE (solo para utilizar con z/OS, Informix, MongoDB, MS SQL SERVER, MYSQL, NETEZZA, Oracle, PostgreSQL, Sybase, TERADATA, VSAM o VSAM COLLECTION PROFILE* (solo para utilizar con z/OS). Para las reglas de excepción y extrusión: Cassandra, CIFS, CounchDB, DB2, FTP, GreenPlumDB, Hadoop, IBM INFORMIX (DRDA), IBM iSeries, Informix, MongoDB, MS SQL SERVER, MYSQL, NETEZZA, Oracle, PostgreSQL, Sybase o TERADATA. Nota: Informix da soporte al protocolo SQLEXEC (protocolo nativo de Informix) o DRDA (protocolo de IBM). Estos protocolos se identifican automáticamente para el tráfico de Informix sin más configuración. El atributo Tipo de servidor mostrará INFORMIX (para el protocolo SQLEXEC) y IBM INFORMIX (DRDA) (para el protocolo DRDA). Nota: TERADATA ofrece un inicio de sesión silencioso y permite que los clientes se reconecten de forma automática. Para bloquear las sentencias de Teradata en una política, utilice la función de cortafuegos de S-TAP con el estado ACTIVADO predeterminado y no observe a los usuarios de confianza.
Usuario de BD	Usuario de base de datos. Consulte Especificación de valores y/o grupos de valores en reglas.
Código de error	Código de error (para una excepción). Consulte Especificación de valores y/o grupos de valores en reglas.
Tipo de excepción	Tipo de excepción (seleccionado desde la lista). Nota: Una sesión cerrada por el tiempo de espera excedido de la interfaz gráfica de usuario, en una regla de excepción, no generará un error de sesión (Session_Error).
Nombre de campo	Nombre del campo. Consulte Especificación de valores y/o grupos de valores en reglas. Si se selecciona el recuadro Todo, cada campo de la sentencia SQL debe ser un miembro del grupo.
Rec. mín.	Recuento del número mínimo de veces que la condición en la regla debe coincidir antes que se satisfaga la regla (dependiendo del Intervalo de restablecimiento).
Protocolo de red	Protocolo de red. Consulte Especificación de valores y/o grupos de valores en reglas.

Campo	Descripción
Objeto	Nombre del objeto. Consulte Especificación de valores y/o grupos de valores en reglas. Para Sybase y MS SQL Server, hay dos grupos, MASKED_SP_EXECUTIONS_SYBASE y MASKED_SP_EXECUTIONS_MS_SQL_SERVER respectivamente que incluyen nombres de procedimientos almacenados. Si hay una ejecución de un procedimiento incluido se enmascará todo. Si se selecciona el recuadro Todo, cada campo de la sentencia SQL debe ser un miembro del grupo.
Grupo de objetos/mandatos	Coincidencia con un miembro del grupo de mandatos/objetos seleccionado.
Grupo de objetos/campos	Coincidencia con un miembro del grupo de objetos/campos seleccionado.
Usuario de SO	Usuario del sistema operativo. Consulte Especificación de valores y/o grupos de valores en reglas.
Patrón	Expresión regular de coincidencia, en el recuadro Patrón. Puede especificar una expresión regular manualmente, o pulsar el botón (Expresión regular) para abrir la herramienta Crear expresión regular, que permite especificar y probar expresiones regulares.
Periodo de tiempo	Para hacer que la regla sea sensible a un periodo de tiempo individual, seleccione un periodo de tiempo predefinido de la lista Periodo o pulse el botón (Periodo) para definir un nuevo periodo de tiempo.
Val. Grab.	Cuando se marca, la construcción real que hace que se satisfaga la regla se registrará, y estará disponible en los informes, en el atributo Serie SQL. En el caso de infracción de política, si no se marca, no se registrarán sentencias SQL.
Umbral de registros afectados	Solo para reglas de acceso. Establece un valor de umbral para los registros coincidentes. Ejemplo: Permitir 1000 instancias antes de emprender una acción. Este campo afecta a la salida de la regla en lugar de a la definición de la regla (es decir, qué sucede cuando se desencadena, en lugar de cuándo se debería desencadenar). El umbral de registros afectados se basa en la regla y en la sesión. Las filas devueltas se acumulan desde todas las consultas que satisfacen la condición de la regla. Una vez todos los registros acumulados alcanzan el umbral, se desencadenará la regla y los registros afectados en la sentencia (si la acción es registrar detalles completos) serán el valor acumulado de los registros afectados.
Carácter de reemplazamiento	Define el carácter de enmascaramiento. Cuando la salida de la regla de extrusión coincida con la expresión regular, las partes que coincidan con las subexpresiones entre paréntesis '(' y ')' serán reemplazadas con el carácter de enmascaramiento.
Intervalo de restablecimiento	Se utiliza únicamente si el campo Rec. mín. es mayor que cero. Este valor es el número de minutos después del cual el contador de condición se restablecerá a cero.
Revocar	Este recuadro de selección solo aparece en las reglas de extrusión. Permite excluir de registrar una respuesta que ya se ha seleccionado para su registro mediante una regla anterior de la política. En la mayoría de los casos, puede conseguir el mismo resultado de forma más simple definiendo una sola regla con una o más condiciones NO para excluir las respuestas que no desea y registrando las restantes que satisfacen la regla.
Descripción de regla	Nombre de la regla. Para utilizar una prueba de patrón especial en la regla, especifique el nombre de prueba de patrón especial seguido de un espacio y uno o más caracteres adicionales para hacer que el nombre de regla sea exclusivo, por ejemplo: guardium://SSEC_NUMBER employee. (Consulte Pruebas de patrones especiales para obtener más información). Cuando se visualiza, el nombre irá precedido por el número de regla y la etiqueta Regla de acceso, Regla de excepción o Regla de extrusión, para identificar el tipo de regla. Si la regla se generó con la función Sugerir desde BD, el nombre generado tiene el formato: Regla sugerida <n>_mm-dd hh:mm, con los siguientes componentes n es el número de secuencia para la regla generada mm-dd es el mes y el día en que se generó la regla hh:mm es la hora en que se generó la regla
IP de servidor	Deseleccione el recuadro No para incluir, o marque el recuadro No para excluir: • Cualquier servidor: Deje todos los campos de servidor en blanco. El recuento se incrementará cada vez que un servidor satisfaga la regla. (No puede dejar todos los campos en blanco si el recuadro No está marcado). • Todos los servidores seleccionados por una dirección y máscara IP: Especifique una dirección IP de servidor en el primer recuadro y la máscara de red en el segundo recuadro. El recuento se incrementará cada vez que cualquiera de los servidores especificados satisfaga la regla. Por ejemplo, para seleccionar todos los servidores en la subred 192.168.3.x, especifique 192.168.3.1 en el primer recuadro y 255.255.255.0 en el segundo recuadro. • Un grupo de servidores: Seleccione un grupo de direcciones IP de servidor en la lista desplegable de Grupo o pulse el botón Grupos para definir un grupo nuevo y, a continuación, seleccionar dicho grupo. El recuento se incrementará cada vez que un miembro del grupo especificado satisfaga la regla. • Todos los servidores seleccionados por una dirección y máscara IP Y un grupo de servidores: Utilice los campos IP de servidor y Grupo. El recuento se incrementará cada vez que un servidor especificado utilizando cualquiera de los dos métodos satisface la regla. Comodines permitidos en la dirección de IP. El comodín % está permitido en una política para un grupo de IP de servidor.
Nombre de servicio	Nombre del servicio. Consulte Especificación de valores y/o grupos de valores en reglas.
Gravedad	Seleccione un código de gravedad de la lista: INFORMACIÓN, BAJA, NINGUNA, MEDIA o ALTA. Si se selecciona ALTA y la regla envía alertas de correo electrónico, el correo electrónico se marcará como Urgente.

Campo	Descripción
Patrón de SQL	Expresión regular de coincidencia, en el recuadro Patrón. Puede especificar una expresión regular de forma manual, o pulsar Expresión regular para abrir la herramienta Crear expresión regular, que permite especificar y probar expresiones regulares. Restricción: No se da soporte al Patrón de SQL para reglas de redacción.
Aplicación fuente	Programa fuente de aplicación. Consulte Especificación de valores y/o grupos de valores en reglas.
Desencadenar una vez por sesión	La sesión no se analiza para la misma regla después de la primera coincidencia. Especialmente eficaz para las políticas de "Auditoría selectiva".
Patrón XML	Expresión regular de coincidencia, en el recuadro Patrón. Puede especificar una expresión regular de forma manual, o pulsar Expresión regular para abrir la herramienta Crear expresión regular, que permite especificar y probar expresiones regulares. En este recuadro se puede utilizar una expresión regular de coincidencia. La expresión regular se debe especificar manualmente.
Valores de retorno Full_SQL al utilizar MSSQL	En MSSQL, se utilizan los procedimientos almacenados sp_cursoropen y sp_cursorfetch para consultas de base de datos SELECT. Sp_cursoropen aloja la sentencia original, mientras que el valor de retorno FULL_SQL en una regla de extrusión aparecerá como sp_cursorfetech en lugar de Select * from _____.

Tema principal: Políticas

Integración de reglas personalizadas con políticas de Guardium

Este tema muestra cómo modificar/derivar automáticamente políticas de Guardium desde un sistema de titularidad personalizado.

Este ejemplo tomará una tabla Oracle de ejemplo (CUSTOM_ENTITLEMENT) como un ejemplo de datos de titularidad personalizados, utilizará un script de Oracle para seleccionar datos de esta tabla y, a continuación, generará un archivo con mandatos GuardAPI. El archivo incluirá mandatos para crear o modificar reglas de política nuevas o existentes, cambiar el orden de las reglas de política y reinstalar políticas. Mostraremos cómo ejecutar el script generado y, a continuación, veremos los cambios de política en la interfaz gráfica de usuario de Guardium.

Valor añadido: La API de Guardium proporciona acceso a la funcionalidad de Guardium desde la línea de mandatos o desde un script. Esto permite la automatización de tareas repetitivas, lo que es especialmente útil en implementaciones más grandes. La llamada a estas funciones de GuardAPI permiten que un usuario realice rápidamente operaciones tales como las de mantenimiento de políticas de Guardium.

Siga estos pasos.

1. Defina una estructura de reglas que registra detalles completos para todos los mandatos de manipulación de bases de datos (DML). Se utilizará como plantilla para crear nuevas reglas de creación. La regla pertenecerá a la política de plantilla.
2. Cree el script de Oracle que generará un archivo con los siguientes mandatos de GuardAPI:
    - copy_rule - añade reglas nuevas a las políticas instaladas como una copia de la plantilla de regla
    - update_rule - actualizar las reglas copiadas con los datos relevantes desde la tabla de Oracle y CUSTOM_ENTITLEMENT
    - update_rule - actualiza la regla existente con los datos desde dicha tabla
    - change_rule_order - cambia la posición de la regla
    - policy_install, reinstall_policy – instala / vuelve a instalar políticas
3. Ejecute el script generado.
4. Visualice los cambios de política instalados.

Pasos:

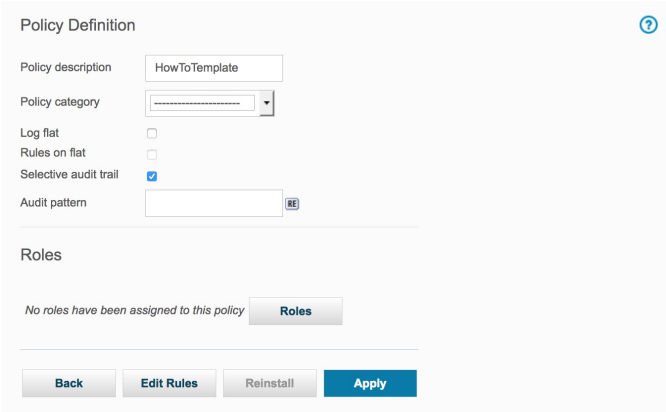
1. Definir una plantilla de regla

    Puesto que se permiten muchas acciones para una regla de política dada, se hace muy difícil definir la estructura jerárquica compleja que una regla tiene utilizando la API Guard. Sin embargo, en la mayoría de los casos, las reglas que difieren por las condiciones y las estructuras de acción/receptor normalmente corresponden a un conjunto pequeño de opciones distintas. Por lo tanto, las API se basan en la clonación de una regla existente que actúa como una plantilla de regla - esto define la estructura de acción/receptor y, a continuación, las condiciones se cambian utilizando las API.

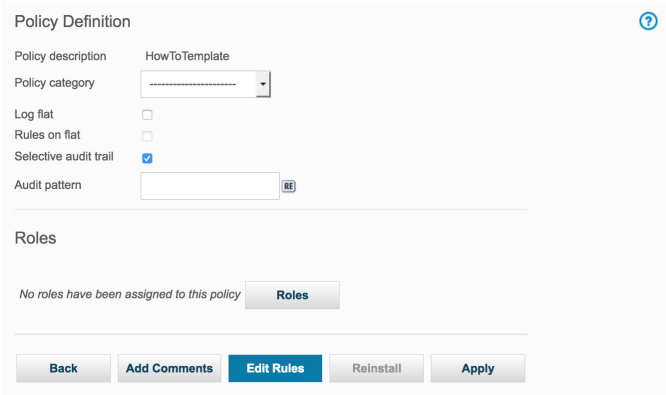
    Aquí crearemos una plantilla de regla (HowToTemplate), que incluirá la definición de la acción de regla y, a continuación, se clonará y actualizará cada vez que se tenga que añadir una regla nueva de este tipo a una política.

    Pulse Proteger > Políticas de seguridad > Creador de políticas para abrir el Buscador de políticas y crear una política de plantilla.

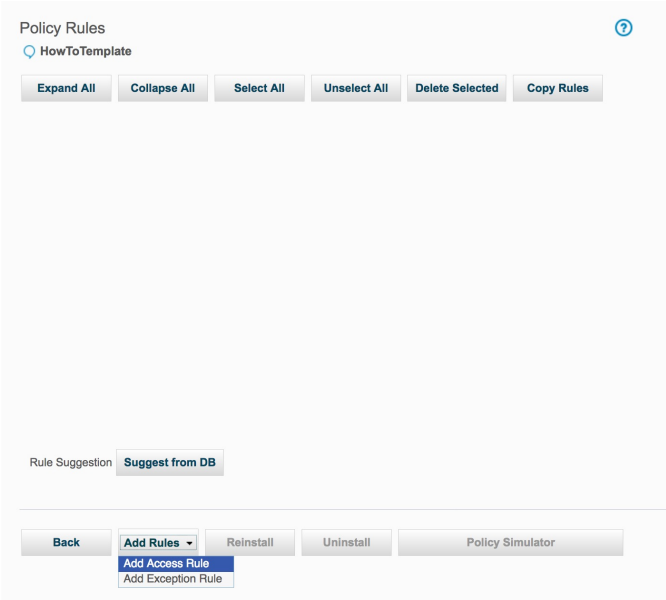
    Pulse Nuevo para crear la política de plantilla. Especifique una descripción de plantilla, seleccione el recuadro de selección Seguimiento de auditoría selectivo y pulse el botón Guardar.



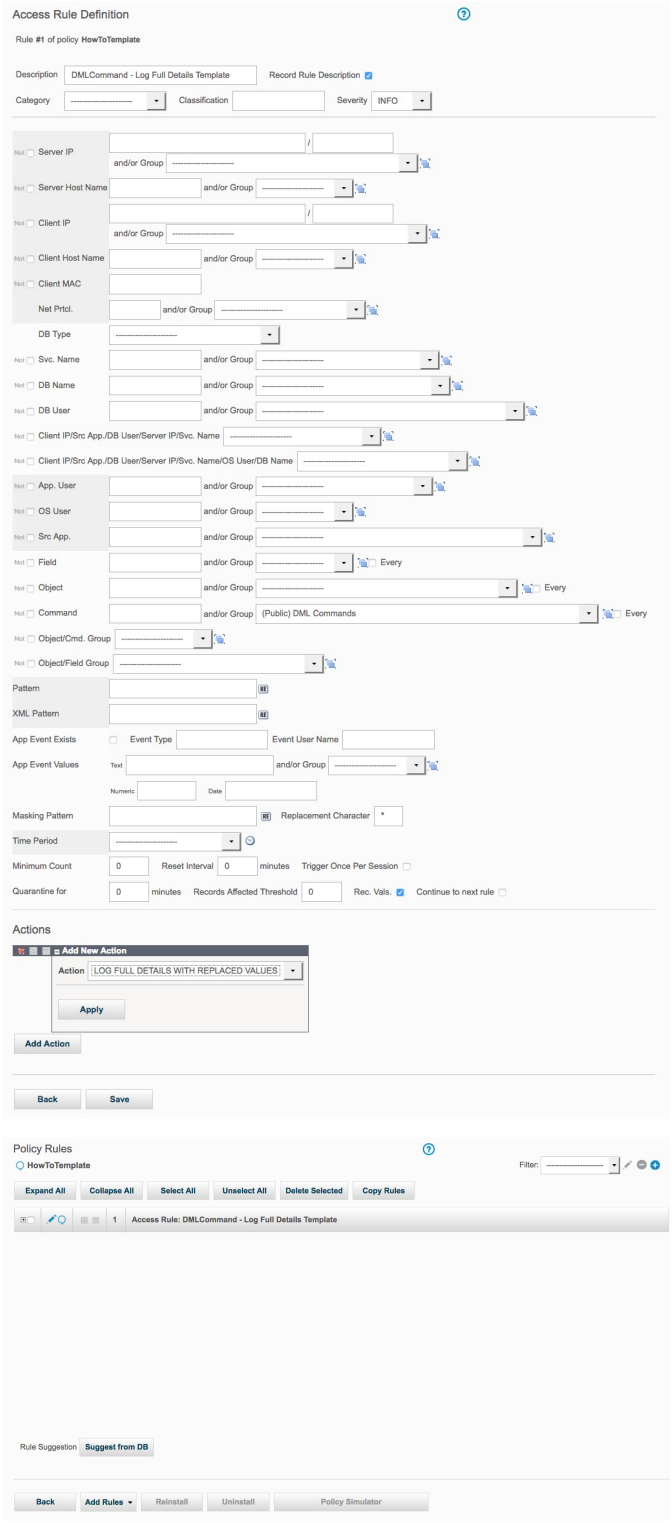
Pulse el botón Editar reglas para añadir una regla de plantilla a esta política



Pulse en el botón **Añadir regla de acceso** para visualizar el panel Definición de regla de acceso y añada una regla.



Para añadir una regla, especifique **DML Command - Log Full Details Template** en el recuadro de Descripción; elija **(Público) Mandatos DML** del recuadro de Mandatos; resalte **REGISTRAR TODOS LOS DETALLES CON VALORES** en la sección Acción y, a continuación, pulse el botón **Guardar**.



2. Cree el script de Oracle que generará un archivo con los mandatos de GuardAPI.

   Elementos clave a saber antes de escribir el script:

   - GuardAPI es un conjunto de mandatos de CLI, que empiezan con la palabra clave **grdapi**. Para listar todos los mandatos GuardAPI disponibles, especifique el mandato 'grdapi' sin argumentos. Para visualizar los parámetros de un mandato determinado, especifique el mandato seguido de '-- help = yes'.

   Por ejemplo

   CLI>grdapi copy_rule --help=yes

   ID=0

   Parámetros de función:

   fromPolicy - obligatorio

   ruleDesc - obligatorio

toPolicy - obligatorio

ok

- Tanto los componentes de palabra clave y valor de los parámetros son sensibles a mayúsculas y minúsculas.
- Si un valor de parámetro contiene uno o varios espacios, se debe delimitar con comillas dobles. Por ejemplo:

```
grdapi copy_rule ruleDesc="DMLCommand - Log Full Details Template" ...
```

- No hay la necesidad de utilizar todos los parámetros disponibles a los que una función da soporte. Además de los parámetros necesarios, utilice los parámetros que desee cambiar.
- Los scripts, que invocan a GuardAPI, pueden contener información confidencial como, por ejemplo, contraseñas para orígenes de datos. Para asegurarse de que la información confidencial se mantiene cifrada en todo momento, el mandato **grdapi** soporta el paso de un parámetro cifrado a una función de API. Este cifrado se realiza utilizando el Secreto compartido del sistema establecido por el administrador y se puede compartir entre distintos sistemas, y entre todas las unidades de un clúster de agregación y/o un gestor central; permitiendo que los scripts con parámetros cifrados se ejecuten en máquinas que tienen el mismo secreto compartido. Para obtener más detalles sobre este aspecto, consulte la ayuda de Guardium.
- Si se instalan varias políticas, entonces el mandato de instalación de política (**policy_install**) debe incluir todas las descripciones de política instaladas delimitadas por una barra vertical. Esto se debe realizar incluso si sólo hay cambios en una política. Las descripciones de política deben estar en el orden en el que desea que se instalen las políticas.

Ejemplo del mandato para la instalación de las políticas HowTo 1 y HowTo 2:

```
grdapi policy_install policy="HowTo 1|HowTo 2"
```

Lógica del script: Cambiar la política HowTo instalada actualmente de la siguiente manera:

a. Para cada registro en la tabla CUSTOM_ENTITLEMENT con IS_NEW_FLAG igual a '1', se añadirá a la política "HowTo" una nueva regla de acceso con descripción guardada en la columna RULE_DESC. La regla registra detalles completos de todos los mandatos DML del usuario de SO (Valor de campo OS_USER), IP de cliente (CLIENT_IP), IP de servidor (SERVER_IP) con el nombre de servicio (SERVICE_NAME).

b. Si el valor de IS_NEW_FLAG es '0', la regla con la descripción igual a la del valor de la columna RULE_DESC se cambiará en base a los correspondientes datos desde este registro de la tabla.

c. Se establecerá a Rule3 como la primera regla, para mostrar cómo utilizar la función **change_rule_order**.

d. Para poder aplicar todos los cambios, se reinstalará la política.

Datos en la tabla custom_entitlement

Tabla 1. Titularidad personalizada

os_user	client_ip	server_ip	rule_desc	service_name	is_new_rule	seq
User1	192.168.7.101	192.168.7.201	Rule1	PROD1	1	1
User2	192.168.7.102	192.168.7.202	Rule2	PROD2	1	2
User3	192.168.7.103	192.168.7.203	Rule3	PROD3	1	3
User4	192.168.7.104	192.168.7.204	Rule2	PROD4	0	4

Los cambios, en base a la lógica y a los datos de la tabla, serán:

a. Añadir una nueva regla de acceso: Rule1. La regla registra detalles completos de todos los mandatos DML desde el usuario "user1", cliente IP "192.168.7.101" en la base de datos Oracle en el servidor "192.168.7.201" con el nombre de servicio "PROD1".

b. Añadir una nueva regla de acceso: Rule2. La regla registra detalles completos de todos los mandatos DML desde el usuario "user2", cliente IP "192.168.7.102" en la base de datos Oracle en el servidor "192.168.7.202" con el nombre de servicio "PROD2".

c. Añadir una nueva regla de acceso: Rule3. La regla registra detalles completos de todos los mandatos DML desde el usuario "user3", cliente IP "192.168.7.103" en la base de datos Oracle en el servidor "192.168.7.203" con el nombre de servicio "PROD3".

d. Cambiar Rule2 – establecer el usuario de SO en "user4", IP de cliente en "192.168.7.104", IP de servidor en "192.168.7.204", nombre de servicio en "PROD4".

e. Establecer a Rule3 como la primera regla en la política.

f. Con objeto de aplicar todos los cambios, vuelve a instalar la política

Script de Oracle

```
SET LINESIZE 2000
SET TERMOUT OFF
SET FEEDBACK OFF

SET SERVEROUTPUT ON SIZE 1000000
spool update_policy.txt

declare cursor CUSTOM_TABLE is
select OS_USER,CLIENT_IP,SERVER_IP,SERVICE_NAME,RULE_DESC,IS_NEW_RULE
  from CUSTOM_ENTITLEMENT order by SEQ;
S_RULE_DESC VARCHAR2(100);
BEGIN
    FOR CUR_W IN CUSTOM_TABLE
    LOOP
        IF NVL(CUR_W.IS_NEW_RULE,'0') = '1' THEN
           -- copy rule
```

```
            DBMS_OUTPUT.PUT_LINE('grdapi copy_rule ruleDesc="DMLCommand - Log Full Details Template" fromPolicy=HowToTemplate
toPolicy=HowTo ');
            S_RULE_DESC := 'DMLCommand - Log Full Details Template';
         ELSE
            S_RULE_DESC := CUR_W.RULE_DESC;
         END IF;
         -- update rule
         DBMS_OUTPUT.PUT_LINE(
         'grdapi update_rule ruleDesc="'||S_RULE_DESC||'"'||
         ' fromPolicy=HowTo newDesc="'|| CUR_W.RULE_DESC ||'" clientIP='||CUR_W.CLIENT_IP ||
         ' clientNetMask=255.255.255.0 serverIP='||CUR_W.SERVER_IP||' serverNetMask=255.255.255.0 '||
         ' serviceName='||CUR_W.SERVICE_NAME ||' osUser='||CUR_W.OS_USER||' dbType=ORACLE');
    END LOOP;
    -- set Rule3 to be the first one
    DBMS_OUTPUT.PUT_LINE('grdapi change_rule_order ruleDesc=Rule3 fromPolicy=HowTo order=1');
    -- reinstall policy
    DBMS_OUTPUT.PUT_LINE('grdapi policy_install policy=HowTo');
END;
/
spool off
```

Script generado con mandatos de GuardAPI

Cuando el script de Oracle se ejecuta dentro SQL*Plus, y se procesa en spool, creará un archivo (update_policy.txt) que será similar a:

```
grdapi copy_rule ruleDesc="DMLCommand - Log Full Details Template" fromPolicy=HowToTemplate toPolicy=HowTo
grdapi update_rule ruleDesc="DMLCommand - Log Full Details Template" fromPolicy=HowTo newDesc="Rule1" clientIP=192.168.7.101
clientNetMask=255.255.255.0 serverIP=192.168.7.201 serverNetMask=255.255.255.0  serviceName=PROD1 osUser=user1 dbType=ORACLE
grdapi copy_rule ruleDesc="DMLCommand - Log Full Details Template" fromPolicy=HowToTemplate toPolicy=HowTo
grdapi update_rule ruleDesc="DMLCommand - Log Full Details Template" fromPolicy=HowTo newDesc="Rule2" clientIP=192.168.7.102
clientNetMask=255.255.255.0 serverIP=192.168.7.202 serverNetMask=255.255.255.0  serviceName=PROD2 osUser=user2 dbType=ORACLE
grdapi copy_rule ruleDesc="DMLCommand - Log Full Details Template" fromPolicy=HowToTemplate toPolicy=HowTo
grdapi update_rule ruleDesc="DMLCommand - Log Full Details Template" fromPolicy=HowTo newDesc="Rule3" clientIP=192.168.7.103
clientNetMask=255.255.255.0 serverIP=192.168.7.203 serverNetMask=255.255.255.0  serviceName=PROD3 osUser=user3 dbType=ORACLE
grdapi update_rule ruleDesc="Rule2" fromPolicy=HowTo newDesc="Rule2" clientIP=192.168.7.104 clientNetMask=255.255.255.0
serverIP=192.168.7.204 serverNetMask=255.255.255.0  serviceName=PROD4 osUser=user4 dbType=ORACLE
grdapi change_rule_order ruleDesc=Rule3 fromPolicy=HowTo order=1
grdapi policy_install policy=HowTo
```

Nota: El último mandato grdapi vuelve a instalar la política para aplicar las reglas al sistema

3. Ejecute el script generado.

   Para ejecutar este script, utilice la estructura de mandatos siguiente:

   ssh cli@[Nombre de dispositivo Guardium] < [nombre script]

   Por ejemplo, para ejecutar el script update_policy.txt en el host 192.168.12.5 (se solicitará una contraseña para el mismo)

   ssh cli@192.168.12.5 <update_policy.txt

   Salida de ejemplo:

   192.168.12.5> ok

   ID=20002

   192.168.12.5> 192.168.12.5> ok

   ID=20015

   192.168.12.5> 192.168.12.5> ok

   ID=20002

   192.168.12.5> 192.168.12.5> ok

   ID=20016

   192.168.12.5> 192.168.12.5> ok

   ID=20002

   192.168.12.5> 192.168.12.5> ok

   ID=20017

   192.168.12.5> 192.168.12.5> ok

   ID=20016

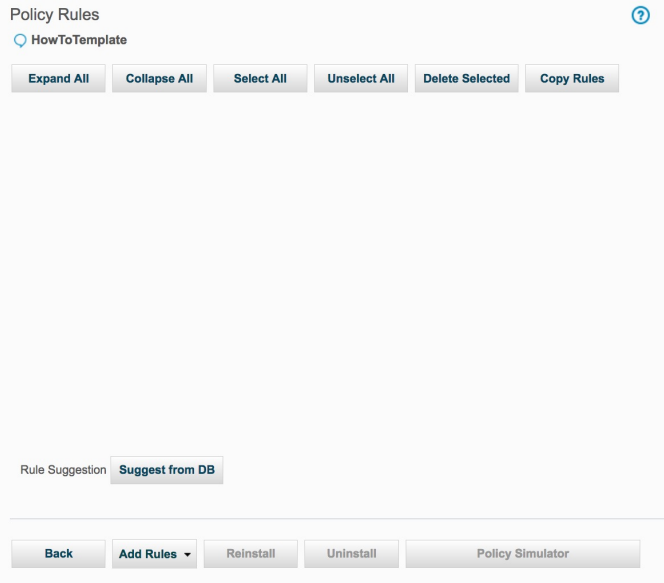
   192.168.12.5> 192.168.12.5> ok

   ID=20002

   192.168.12.5> 192.168.12.5>

4. Visualice los cambios de política instalados.

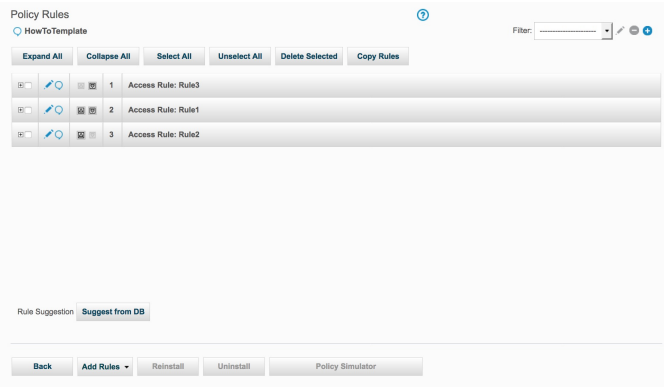
   Antes de ejecutar el script, no habían definidas reglas en la política HowTo tal como se mostraba en esta vista previa



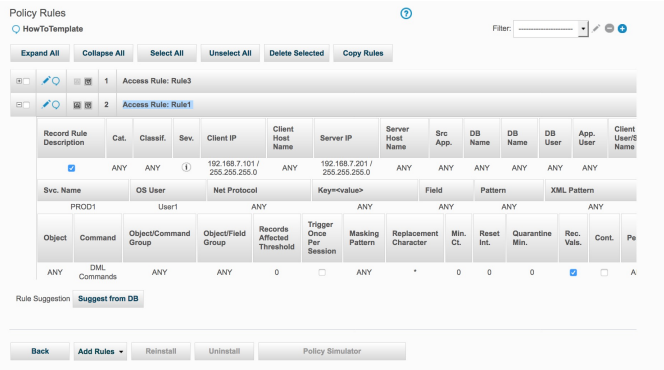
Después de ejecutar el script:

Como resultado de **copy_rule**, ahora la política HowTo tendrá tres reglas de acceso.

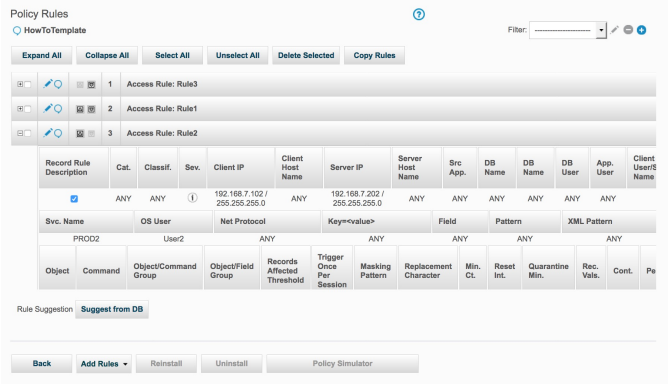
Como resultado del mandato **change_rule_order**, Rule3 estará en primer lugar.



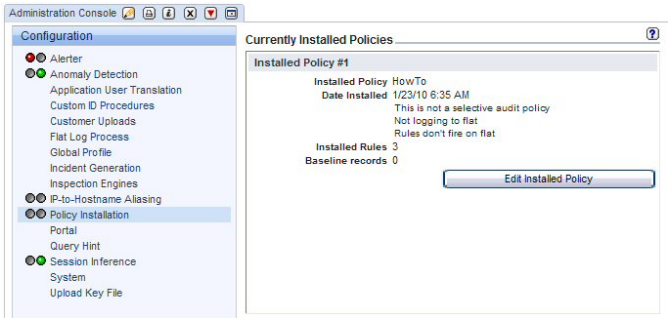
Expandiendo cualquiera de las reglas de política, Rule1 aquí, podemos validar los diversos campos que se han modificado con los mandatos **update_rule**.



Como resultado del mandato **update_rule**, se ha cambiado la Rule2.



Y como resultado del mandato **policy_install**, la política instalada actualmente es ahora la política HowTo con tres reglas instaladas.



Tema principal: Políticas

Utilización de la acción Ignorar adecuada

En este tema se explica cómo se manejan los datos al utilizar acciones de Ignorar en reglas de política.

Valor-añadido: Conocer con mayor precisión lo que ocurre cuando se realizan determinadas elecciones en Reglas de política para acciones de registrar o ignorar, que controlan el nivel de registro, en función del tráfico observado.

Para obtener más información, consulte Políticas.

Ignorar sesión

Se ignora la solicitud actual y el resto de la sesión. Esta acción no registra una infracción de política, pero detiene el registro de las construcciones y no realizará pruebas para verificar infracciones de política de ningún tipo durante el resto de la sesión. Esta acción podría ser útil si, por ejemplo, la base de datos incluye una región de prueba, y no hay una necesidad de aplicar reglas de política en esa región de la base de datos.

Tabla 1. Ignorar sesión

Datos registrados o ignorados entre el cliente y el servidor de BD/S-TAP	**Datos enviados desde el servidor de DB/S-TAP al recopilador**	**Datos desde el puerto Span/TAP de red al recopilador**
Ignorar - Mandatos SQL, Errores SQL, Conjuntos de resultados	Iniciar sesión / Finalizar sesión Sniffer a S-TAP - Una señal a S-TAP para que deje de enviar actividad para esta sesión. Si S-TAP envía actividad adicional, se ignora únicamente a nivel de sniffer. Ignorar mandatos SQL Ignorar errores de SQL Ignorar conjuntos de resultados	Ignorar – Mandatos SQL, Errores SQL, Conjuntos de resultados. Los mandatos y errores SQL provenientes desde un TAP de red o Puerto de Span se filtran en el sniffer.

Ignorar sesión S-TAP

Se ignora la solicitud actual y el resto de la sesión S-TAP. Esta acción se realiza en combinación con la especificación en la pantalla del menú del creador de políticas de determinadas máquinas, usuarios o aplicaciones que están produciendo un gran volumen de tráfico de red. Esta acción es útil en los casos en los que sabe que la respuesta de la base de datos de la sesión de S-TAP no será de interés.

Tabla 2. Ignorar sesión S-TAP

Datos registrados o ignorados entre el cliente y el servidor de BD/S-TAP	**Datos enviados desde el servidor de DB/S-TAP al recopilador**	**Datos desde el puerto Span/TAP de red al recopilador**

Datos registrados o ignorados entre el cliente y el servidor de BD/S-TAP	Datos enviados desde el servidor de DB/S-TAP al recopilador	Datos desde el puerto Span/TAP de red al recopilador
Ignorar - Mandatos SQL, Errores SQL, Conjuntos de resultados	Iniciar sesión / Finalizar sesión Sniffer a S-TAP - Una señal a S-TAP para que deje de enviar actividad para esta sesión. Se envían señales adicionales a S-TAP para detener el envío de actividad a esta sesión.	No aplicable Si existe la necesidad de ignorar el tráfico de un TAP de red / Puerto Span, utilice en su lugar la Ignorar sesión.

Ignorar respuestas por sesión

Se ignorarán las respuestas para el resto de la sesión. Esta acción registra una infracción de política, pero detiene el análisis de respuestas para el resto de la sesión. Esta acción es útil en los casos en los que sabe que la respuesta de la base de datos no será de interés.

Nota: Para ignorar respuestas por sesión, puesto que el sniffer no recibe respuestas para la consulta o esta se ignora, los valores para COUNT_FAILED y SUCCESS son los que se hayan definido como predeterminados para la tabla, en este caso COUNT_FAILED=0 y SUCCESS=1.

Tabla 3. Ignorar respuestas por sesión

Datos registrados o ignorados entre el cliente y el servidor de BD/S-TAP	Datos enviados desde el servidor de DB/S-TAP al recopilador	Datos desde el puerto Span/TAP de red al recopilador
Registrar – Mandatos SQL Ignorar - Errores SQL, Conjuntos de resultados	Iniciar sesión / Finalizar sesión Mandatos SQL Sniffer a S-TAP - Una señal a S-TAP para que deje de enviar actividad para esta sesión. Se envían señales adicionales a S-TAP para detener el envío de actividad a esta sesión.	No aplicable Esta acción de regla es únicamente para implementaciones S-TAP.

Ignorar SQL por sesión

No se registrará SQL durante el resto de la sesión. Las excepciones se continuarán registrando, sin embargo, el sistema no capturará las series SQL que corresponden a las excepciones.

Tabla 4. Ignorar SQL por sesión

Datos registrados o ignorados entre el cliente y el servidor de BD/S-TAP	Datos enviados desde el servidor de DB/S-TAP al recopilador	Datos desde el puerto Span/TAP de red al recopilador
Ignorar - Mandatos SQL Registrar - Errores SQL, Conjuntos de resultados	Iniciar sesión / Finalizar sesión Sniffer a S-TAP - Una señal a S-TAP para que deje de enviar actividad para esta sesión. Si S-TAP envía actividad adicional, se ignora únicamente a nivel de sniffer. Registrar mandatos SQL Registrar errores SQL Registrar conjuntos de resultados, si se están utilizando reglas de extrusión	Ignorar – Mandatos SQL Registrar - Errores SQL, Conjuntos de resultados Los mandatos SQL se filtran en el Sniffer.

Seguimiento de auditoría selectivo

Utilice una política de Seguimiento de auditoría selectivo para limitar la cantidad de información de registro en el dispositivo. Esto es apropiado cuando el tráfico de interés sea un porcentaje relativamente pequeño del tráfico aceptado por los motores de inspección, o cuando todo el tráfico del que podría querer informar se puede identificar casi de forma completa.

Es importante tener en cuenta que las reglas de Ignorar sesión siguen siendo muy importantes para incluirlas en la política incluso si se utiliza un Seguimiento de auditoría selectivo. Las reglas de Ignorar sesión disminuyen considerablemente la carga en un recopilador al filtrar la información a nivel de S-TAP; el recopilador nunca la recibe y no tiene que consumir recursos analizando el tráfico que al final no se registra. Una política de Seguimiento de auditoría selectivo sin reglas de Ignorar sesión significaría que todo el tráfico se enviaría desde el servidor de base de datos al recopilador, lo que haría que el recopilador tuviese que analizar todos los mandatos y conjuntos de resultados generados por el servidor de base de datos.

Tabla 5. Seguimiento de auditoría selectivo

Datos registrados o ignorados entre el cliente y el servidor de BD/S-TAP	Datos enviados desde el servidor de DB/S-TAP al recopilador	Datos desde el puerto Span/TAP de red al recopilador
Ignorar - Mandatos SQL Registrar - Errores SQL, Conjuntos de resultados	Iniciar sesión / Finalizar sesión Ignorar mandatos SQL, excepto aquellos definidos mediante reglas de Solo auditoría o Detalles detalles completos. Registrar errores SQL Registrar conjuntos de resultados, si se están utilizando reglas de extrusión	Ignorar – Mandatos SQL Registrar - Errores SQL, Conjuntos de resultados Los mandatos SQL se filtran en el Sniffer.

Tema principal: Políticas

Conjuntos de caracteres

Los códigos de los conjuntos de caracteres se utilizan en las reglas de extrusión.

Lista de códigos de conjuntos de caracteres posibles

ANSI_X3.4-1968 - 1
ANSI_X3.4-1986 - 2
ASCII - 3
CP367 - 4
IBM367 - 5
ISO-IR-6 - 6
ISO646-US - 7
ISO_646.IRV:1991 - 8
US - 9
US-ASCII - 10
CSASCII - 11
UTF-8 - 12
ISO-10646/UCS2 - 13
UCS-2 - 14
CSUNICODE - 15
UCS-2BE - 16
UNICODE - 17
UNICODEBIG - 18
TSCII - 19
UCS-2LE - 20
UNICODELITTLE - 21
ISO-10646/UCS4 - 22
UCS-4 - 23
CSUCS4 - 24
UCS-4BE - 25
UCS-4LE - 26
UTF-16 - 27
UTF-16BE - 28
UTF-16LE - 29
UTF-32 - 30
UTF-32BE - 31
UTF-32LE - 32
UTF7 - 33
UTF-7 - 34
UTF-8 - 35
UCS2 - 36
UCS2 - 37
UCS4 - 38
UCS4 - 39
UTF8 - 40
UTF8 - 41
CP819 - 42
IBM819 - 43
ISO-8859-1 - 44
ISO-IR-100 - 45
ISO8859-1 - 46
ISO_8859-1 - 47
ISO_8859-1:1987 - 48
L1 - 49
LATIN1 - 50
CSISOLATIN1 - 51
ISO-8859-2 - 52
ISO-IR-101 - 53
ISO8859-2 - 54
ISO_8859-2 - 55
ISO_8859-2:1987 - 56
L2 - 57
LATIN2 - 58
CSISOLATIN2 - 59
ISO-8859-3 - 60
ISO-IR-109 - 61
ISO8859-3 - 62
ISO_8859-3 - 63
ISO_8859-3:1988 - 64
L3 - 65
LATIN3 - 66
CSISOLATIN3 - 67
ISO-8859-4 - 68
ISO-IR-110 - 69
ISO8859-4 - 70
ISO_8859-4 - 71
ISO_8859-4:1988 - 72
L4 - 73
LATIN4 - 74
CSISOLATIN4 - 75

CYRILLIC - 76
ISO-8859-5 - 77
ISO-IR-144 - 78
ISO8859-5 - 79
ISO_8859-5 - 80
ISO_8859-5:1988 - 81
CSISOLATINCYRILLIC - 82
ARABIC - 83
ASMO-708 - 84
ECMA-114 - 85
ISO-8859-6 - 86
ISO-IR-127 - 87
ISO8859-6 - 88
ISO_8859-6 - 89
ISO_8859-6:1987 - 90
CSISOLATINARABIC - 91
ECMA-118 - 92
ELOT_928 - 93
GREEK - 94
GREEK8 - 95
ISO-8859-7 - 96
ISO-IR-126 - 97
ISO8859-7 - 98
ISO_8859-7 - 99
ISO_8859-7:1987 - 100
CSISOLATINGREEK - 101
HEBREW - 102
ISO-8859-8 - 103
ISO-IR-138 - 104
ISO8859-8 - 105
ISO_8859-8 - 106
ISO_8859-8:1988 - 107
CSISOLATINHEBREW - 108
ISO-8859-9 - 109
ISO-IR-148 - 110
ISO8859-9 - 111
ISO_8859-9 - 112
ISO_8859-9:1989 - 113
L5 - 114
LATIN5 - 115
CSISOLATIN5 - 116
ISO-8859-10 - 117
ISO-IR-157 - 118
ISO8859-10 - 119
ISO_8859-10 - 120
ISO_8859-10:1992 - 121
L6 - 122
LATIN6 - 123
CSISOLATIN6 - 124
ISO-8859-13 - 125
ISO-8859-13 - 126
ISO-8859-13 - 127
ISO-8859-13 - 128
L7 - 129
LATIN7 - 130
ISO-8859-14 - 131
ISO-CELTIC - 132
ISO-IR-199 - 133
ISO8859-14 - 134
ISO_8859-14 - 135
ISO_8859-14:1998 - 136
L8 - 137
LATIN8 - 138
ISO-8859-15 - 139
ISO-IR-203 - 140
ISO8859-15 - 141
ISO_8859-15 - 142
ISO_8859-15:1998 - 143
ISO-8859-16 - 144
ISO-IR-226 - 145
ISO8859-16 - 146
ISO_8859-16 - 147
ISO_8859-16:2000 - 148
KOI8-R - 149
CSKOI8R? - 150
KOI8U? - 151
KOI8R? - 152
CP1250 - 153
MS-EE - 154
WINDOWS-1250 - 155

CP1251 - 156
MS-CYRL - 157
WINDOWS-1251 - 158
CP1252 - 159
MS-ANSI - 160
WINDOWS-1252 - 161
CP1253 - 162
MS-GREEK - 163
WINDOWS-1253 - 164
CP1254 - 165
MS-TURK - 166
WINDOWS-1254 - 167
CP1255 - 168
MS-HEBR - 169
WINDOWS-1255 - 170
CP1256 - 171
MS-ARAB - 172
WINDOWS-1256 - 173
CP1257 - 174
WINBALTRIM - 175
WINDOWS-1257 - 176
CP1258 - 177
WINDOWS-1258 - 178
850 - 179
CP850 - 180
IBM850 - 181
CSPC850MULTILINGUAL? - 182
862 - 183
CP862 - 184
IBM862 - 185
CSPC862LATINHEBREW? - 186
866 - 187
CP866 - 188
IBM866 - 189
CSIBM866 - 190
MAC - 191
MACINTOSH - 192
MACUK - 193
CSMACINTOSH - 194
MACIS - 195
MAC - 196
MAC - 197
MAC - 198
MAC - 199
MACUKRAINIAN - 200
MAC - 201
MAC - 202
MAC - 203
MAC - 204
MAC - 205
HP-ROMAN8 - 206
R8 - 207
ROMAN8 - 208
HPROMAN8 - 209
ROMAN8 - 210
ARMSCII-8 - 211
GEORGIAN-ACADEMY - 212
GEORGIAN-PS - 213
KOI8-T - 214
KOI8-T - 215
CP1133 - 216
IBM-CP1133 - 217
ISO-IR-166 - 218
TIS-620 - 219
TIS620 - 220
TIS620-0 - 221
TIS620.2529-1 - 222
TIS620.2533-0 - 223
TIS620.2533-1 - 224
CP874 - 225
WINDOWS-874 - 226
VISCII - 227
VISCII - 228
VISCII - 229
TCVN - 230
TCVN-5712 - 231
TCVN5712-1 - 232
TCVN5712-1:1993 - 233
ISO-IR-14 - 234
ISO646-JP - 235

JIS_C6220-1969-RO - 236
JP - 237
CSISO14JISC6220RO? - 238
JISX0201-1976 - 239
JIS_X0201 - 240
X0201 - 241
CSHALFWIDTHKATAKANA - 242
ISO-IR-87 - 243
JIS0208 - 244
JIS_C6226-1983 - 245
JIS_X0208 - 246
JIS_X0208-1983 - 247
JIS_X0208-1990 - 248
X0208 - 249
CSISO87JISX0208? - 250
ISO-IR-159 - 251
JIS_X0212 - 252
JIS_X0212-1990 - 253
JIS_X0212.1990-0 - 254
X0212 - 255
CSISO159JISX02121990? - 256
CN - 257
GB_1988-80 - 258
ISO-IR-57 - 259
ISO646-CN - 260
CSISO57GB1988? - 261
CHINESE - 262
GB_2312-80 - 263
ISO-IR-58 - 264
CSISO58GB231280? - 265
CN-GB-ISOIR165 - 266
ISO-IR-165 - 267
ISO-IR-149 - 268
KOREAN - 269
KSC_5601 - 270
KS_C_5601-1987 - 271
KS_C_5601-1989 - 272
CSKSC56011987 - 273
EUC-JP - 274
EUCJP - 275
EXTENDED_UNIX_CODE_PACKED_FORMAT_FOR_JAPANESE - 276
CSEUCPKDFMTJAPANESE - 277
MS_KANJI - 278
SHIFT-JIS - 279
SHIFT_JIS - 280
SJIS - 281
CSSHIFTJIS - 282
CP932 - 283
ISO-2022-JP - 284
CSISO2022JP? - 285
ISO-2022-JP-1 - 286
ISO-2022-JP-2 - 287
CSISO2022JP2? - 288
CN-GB - 289
EUC-CN - 290
EUCCN - 291
GB2312 - 292
CSGB2312 - 293
CP936 - 294
GBK - 295
GB18030 - 296
ISO-2022-CN - 297
CSISO2022CN? - 298
ISO-2022-CN-EXT - 299
HZ - 300
HZ-GB-2312 - 301
EUC-TW - 302
EUCTW - 303
CSEUCTW - 304
BIG-5 - 305
BIG-FIVE - 306
BIG5 - 307
BIGFIVE - 308
CN-BIG5 - 309
CSBIG5 - 310
CP950 - 311
BIG5-HKSCS - 312
BIG5HKSCS? - 313
EUC-KR - 314
EUCKR - 315

CSEUCKR - 316
CP949 - 317
UHC - 318
CP1361 - 319
JOHAB - 320
ISO-2022-KR - 321
CSISO2022KR? - 322
IBM037 - 323
IBM038 - 324
IBM256 - 325
IBM273 - 326
IBM274 - 327
IBM275 - 328
IBM277 - 329
IBM278 - 330
IBM280 - 331
IBM281 - 332
IBM284 - 333
IBM285 - 334
IBM290 - 335
IBM297 - 336
IBM367 - 337
IBM420 - 338
IBM423 - 339
IBM424 - 340
IBM437 - 341
IBM500 - 342
IBM775 - 343
IBM813 - 344
IBM819 - 345
IBM848 - 346
IBM850 - 347
IBM851 - 348
IBM852 - 349
IBM855 - 350
IBM856 - 351
IBM857 - 352
IBM860 - 353
IBM861 - 354
IBM862 - 355
IBM863 - 356
IBM864 - 357
IBM865 - 358
IBM866 - 359
IBM866NAV? - 360
IBM868 - 361
IBM869 - 362
IBM870 - 363
IBM871 - 364
IBM874 - 365
IBM875 - 366
IBM880 - 367
IBM891 - 368
IBM903 - 369
IBM904 - 370
IBM905 - 371
IBM912 - 372
IBM915 - 373
IBM916 - 374
IBM918 - 375
IBM920 - 376
IBM922 - 377
IBM930 - 378
IBM932 - 379
IBM933 - 380
IBM935 - 381
IBM937 - 382
IBM939 - 383
IBM943 - 384
IBM1004 - 385
IBM1026 - 386
IBM1046 - 387
IBM1047 - 388
IBM1089 - 389
IBM1124 - 390
IBM1129 - 391
IBM1132 - 392
IBM1133 - 393
IBM1160 - 394
IBM1161 - 395

IBM1162 - 396
IBM1163 - 397
IBM1164 - 398
MSCP949 - 399
EUC-JISX0213 - 400
UJIS - 401
CP852 - 402
EUCJP-MS - 403
IBM902 - 404
IBM921 - 405
WINDOWS-31J - 406
IBM1025 - 407
IBM1140 - 408
IBM1137 - 409
IBM1122 - 410
IBM1141 - 411
IBM1142 - 412
IBM1143 - 413
IBM1144 - 414
IBM1145 - 415
IBM1146 - 416
IBM1147 - 417
IBM1148 - 418
IBM1149 - 419
IBM1153 - 420
IBM1155 - 421
IBM1157 - 422
EBCDICUS - 423
IBM1112 - 424
IBM1158 - 425
437 - 426
500g - 427
500V1g - 428
851g - 429
852g - 430
855g - 431
856g - 432
857g - 433
860g - 434
861g - 435
863g - 436
864g - 437
865g - 438
866NAVg - 439
869g - 440
874g - 441
904g - 442
1026g - 443
1046g - 444
1047g - 445
8859_1g - 446
8859_2g - 447
8859_3g - 448
8859_4g - 449
8859_5g - 450
8859_6g - 451
8859_7g - 452
8859_8g - 453
8859_9g - 454
10646-1:1993g - 455
10646-1:1993/UCS4/ - 456
ANSI_X3.4g - 457
ANSI_X3.110-1983g - 458
ANSI_X3.110g - 459
ARABIC7g - 460
ASMO_449g - 461
BALTICg - 462
BIG-5g - 463
BIG-FIVEg - 464
BIG5-HKSCSg - 465
BIG5g - 466
BIG5HKSCSg? - 467
BIGFIVEg - 468
BS_4730g - 469
CAg - 470
CN-BIG5g - 471
CN-GBg - 472
CNg - 473
CP-ARg - 474
CP-GRg - 475

CP-HUg - 476
CP037g - 477
CP038g - 478
CP273g - 479
CP274g - 480
CP275g - 481
CP278g - 482
CP280g - 483
CP281g - 484
CP282g - 485
CP284g - 486
CP285g - 487
CP290g - 488
CP297g - 489
CP420g - 490
CP423g - 491
CP424g - 492
CP437g - 493
CP500g - 494
CP737g - 495
CP775g - 496
CP803g - 497
CP813g - 498
CP851g - 499
CP852g - 500
CP855g - 501
CP856g - 502
CP857g - 503
CP860g - 504
CP861g - 505
CP863g - 506
CP864g - 507
CP865g - 508
CP866NAVg? - 509
CP868g - 510
CP869g - 511
CP870g - 512
CP871g - 513
CP875g - 514
CP880g - 515
CP891g - 516
CP901g - 517
CP902g - 518
CP903g - 519
CP904g - 520
CP905g - 521
CP912g - 522
CP915g - 523
CP916g - 524
CP918g - 525
CP920g - 526
CP921g - 527
CP922g - 528
CP930g - 529
CP932g - 530
CP933g - 531
CP935g - 532
CP936g - 533
CP937g - 534
CP939g - 535
CP949g - 536
CP950g - 537
CP1004g - 538
CP1008g - 539
CP1025g - 540
CP1026g - 541
CP1046g - 542
CP1047g - 543
CP1070g - 544
CP1079g - 545
CP1081g - 546
CP1084g - 547
CP1089g - 548
CP1097g - 549
CP1112g - 550
CP1122g - 551
CP1123g - 552
CP1124g - 553
CP1125g - 554
CP1129g - 555

CP1130g - 556
CP1132g - 557
CP1137g - 558
CP1140g - 559
CP1141g - 560
CP1142g - 561
CP1143g - 562
CP1144g - 563
CP1145g - 564
CP1146g - 565
CP1147g - 566
CP1148g - 567
CP1149g - 568
CP1153g - 569
CP1154g - 570
CP1155g - 571
CP1156g - 572
CP1157g - 573
CP1158g - 574
CP1160g - 575
CP1161g - 576
CP1162g - 577
CP1163g - 578
CP1164g - 579
CP1166g - 580
CP1167g - 581
CP1361g - 582
CP1364g - 583
CP1371g - 584
CP1388g - 585
CP1390g - 586
CP1399g - 587
CP4517g - 588
CP4899g - 589
CP4909g - 590
CP4971g - 591
CP5347g - 592
CP9030g - 593
CP9066g - 594
CP9448g - 595
CP10007g - 596
CP12712g - 597
CP16804g - 598
CPIBM861g - 599
CSA7-1g - 600
CSA7-2g - 601
CSA_T500-1983g - 602
CSA_T500g - 603
CSA_Z243.4-1985-1g - 604
CSA_Z243.4-1985-2g - 605
CSA_Z243.419851g - 606
CSA_Z243.419852g - 607
CSDECMCSg - 608
CSEBCDICATDEg - 609
CSEBCDICATDEAg - 610
CSEBCDICCAFRg - 611
CSEBCDICDKNOg - 612
CSEBCDICDKNOAg - 613
CSEBCDICESg - 614
CSEBCDICESAg - 615
CSEBCDICESSg - 616
CSEBCDICFISEg - 617
CSEBCDICFISEAg - 618
CSEBCDICFRg - 619
CSEBCDICITg - 620
CSEBCDICPTg - 621
CSEBCDICUKg - 622
CSEBCDICUSg - 623
CSEUCKRg - 624
CSEUCPKDFMTJAPANESEg - 625
CSGB2312g - 626
CSIBM037g - 627
CSIBM038g - 628
CSIBM273g - 629
CSIBM274g - 630
CSIBM275g - 631
CSIBM277g - 632
CSIBM278g - 633
CSIBM280g - 634
CSIBM281g - 635

CSIBM284g - 636
CSIBM285g - 637
CSIBM290g - 638
CSIBM297g - 639
CSIBM420g - 640
CSIBM423g - 641
CSIBM424g - 642
CSIBM500g - 643
CSIBM803g - 644
CSIBM851g - 645
CSIBM855g - 646
CSIBM856g - 647
CSIBM857g - 648
CSIBM860g - 649
CSIBM863g - 650
CSIBM864g - 651
CSIBM865g - 652
CSIBM868g - 653
CSIBM869g - 654
CSIBM870g - 655
CSIBM871g - 656
CSIBM880g - 657
CSIBM891g - 658
CSIBM901g - 659
CSIBM902g - 660
CSIBM903g - 661
CSIBM904g - 662
CSIBM905g - 663
CSIBM918g - 664
CSIBM921g - 665
CSIBM922g - 666
CSIBM930g - 667
CSIBM932g - 668
CSIBM933g - 669
CSIBM935g - 670
CSIBM937g - 671
CSIBM939g - 672
CSIBM943g - 673
CSIBM1008g - 674
CSIBM1025g - 675
CSIBM1026g - 676
CSIBM1097g - 677
CSIBM1112g - 678
CSIBM1122g - 679
CSIBM1123g - 680
CSIBM1124g - 681
CSIBM1129g - 682
CSIBM1130g - 683
CSIBM1132g - 684
CSIBM1133g - 685
CSIBM1137g - 686
CSIBM1140g - 687
CSIBM1141g - 688
CSIBM1142g - 689
CSIBM1143g - 690
CSIBM1144g - 691
CSIBM1145g - 692
CSIBM1146g - 693
CSIBM1147g - 694
CSIBM1148g - 695
CSIBM1149g - 696
CSIBM1153g - 697
CSIBM1154g - 698
CSIBM1155g - 699
CSIBM1156g - 700
CSIBM1157g - 701
CSIBM1158g - 702
CSIBM1160g - 703
CSIBM1161g - 704
CSIBM1163g - 705
CSIBM1164g - 706
CSIBM1166g - 707
CSIBM1167g - 708
CSIBM1364g - 709
CSIBM1371g - 710
CSIBM1388g - 711
CSIBM1390g - 712
CSIBM1399g - 713
CSIBM4517g - 714
CSIBM4899g - 715

CSIBM4909g - 716
CSIBM4971g - 717
CSIBM5347g - 718
CSIBM9030g - 719
CSIBM9066g - 720
CSIBM9448g - 721
CSIBM12712g - 722
CSIBM16804g - 723
CSIBM11621162g - 724
CSISO4UNITEDKINGDOMg? - 725
CSISO10SWEDISHg? - 726
CSISO11SWEDISHFORNAMESg? - 727
CSISO15ITALIANg? - 728
CSISO16PORTUGESEg? - 729
CSISO17SPANISHg? - 730
CSISO18GREEK7OLDg? - 731
CSISO19LATINGREEKg? - 732
CSISO21GERMANg? - 733
CSISO25FRENCHg? - 734
CSISO27LATINGREEK1g? - 735
CSISO49INISg? - 736
CSISO50INIS8g? - 737
CSISO51INISCYRILLICg? - 738
CSISO58GB1988g? - 739
CSISO60DANISHNORWEGIANg? - 740
CSISO60NORWEGIAN1g? - 741
CSISO61NORWEGIAN2g? - 742
CSISO69FRENCHg? - 743
CSISO84PORTUGUESE2g? - 744
CSISO85SPANISH2g? - 745
CSISO86HUNGARIANg? - 746
CSISO88GREEK7g? - 747
CSISO89ASMO449g? - 748
CSISO90g - 749
CSISO92JISC62991984Bg? - 750
CSISO99NAPLPSg? - 751
CSISO103T618BITg? - 752
CSISO111ECMACYRILLICg? - 753
CSISO121CANADIAN1g? - 754
CSISO122CANADIAN2g? - 755
CSISO139CSN369103g? - 756
CSISO141JUSIB1002g? - 757
CSISO143IECP271g? - 758
CSISO150g - 759
CSISO150GREEKCCITTg? - 760
CSISO151CUBAg? - 761
CSISO153GOST1976874g? - 762
CSISO646DANISHg? - 763
CSISO2022CNg? - 764
CSISO2022JPg? - 765
CSISO2022JP2g? - 766
CSISO2022KRg? - 767
CSISO2033g - 768
CSISO5427CYRILLICg? - 769
CSISO5427CYRILLIC1981g? - 770
CSISO5428GREEKg? - 771
CSISO10367BOXg? - 772
CSKSC5636g - 773
CSNATSDANOg - 774
CSNATSSEFIg - 775
CSN_369103g - 776
CSPC8CODEPAGE437g? - 777
CSPC775BALTICg? - 778
CSPCP852g - 779
CSSHIFTJISg - 780
CSUCS4g - 781
CSWINDOWS31Jg? - 782
CUBAg - 783
CWI-2g - 784
CWIg - 785
DEg - 786
DEC-MCSg - 787
DECg - 788
DECMCSg - 789
DIN_66003g - 790
DKg - 791
DS2089g - 792
DS_2089g - 793
E13Bg? - 794
EBCDIC-AT-DE-Ag - 795

EBCDIC-AT-DEg - 796
EBCDIC-BEg - 797
EBCDIC-BRg - 798
EBCDIC-CA-FRg - 799
EBCDIC-CP-AR1g - 800
EBCDIC-CP-AR2g - 801
EBCDIC-CP-BEg - 802
EBCDIC-CP-CAg - 803
EBCDIC-CP-CHg - 804
EBCDIC-CP-DKg - 805
EBCDIC-CP-ESg - 806
EBCDIC-CP-FIg - 807
EBCDIC-CP-FRg - 808
EBCDIC-CP-GBg - 809
EBCDIC-CP-GRg - 810
EBCDIC-CP-HEg - 811
EBCDIC-CP-ISg - 812
EBCDIC-CP-ITg - 813
EBCDIC-CP-NLg - 814
EBCDIC-CP-NOg - 815
EBCDIC-CP-ROECEg - 816
EBCDIC-CP-SEg - 817
EBCDIC-CP-TRg - 818
EBCDIC-CP-USg - 819
EBCDIC-CP-WTg - 820
EBCDIC-CP-YUg - 821
EBCDIC-CYRILLICg - 822
EBCDIC-DK-NO-Ag - 823
EBCDIC-DK-NOg - 824
EBCDIC-ES-Ag - 825
EBCDIC-ES-Sg - 826
EBCDIC-ESg - 827
EBCDIC-FI-SE-Ag - 828
EBCDIC-FI-SEg - 829
EBCDIC-FRg - 830
EBCDIC-GREEKg - 831
EBCDIC-INTg - 832
EBCDIC-INT1g - 833
EBCDIC-IS-FRISSg - 834
EBCDIC-ITg - 835
EBCDIC-JP-Eg - 836
EBCDIC-JP-KANAg - 837
EBCDIC-PTg - 838
EBCDIC-UKg - 839
EBCDIC-USg - 840
EBCDICATDEg - 841
EBCDICATDEAg - 842
EBCDICCAFRg - 843
EBCDICDKNOg - 844
EBCDICDKNOAg - 845
EBCDICESg - 846
EBCDICESAg - 847
EBCDICESSg - 848
EBCDICFISEg - 849
EBCDICFISEAg - 850
EBCDICFRg - 851
EBCDICISFRISSg - 852
EBCDICITg - 853
EBCDICPTg - 854
EBCDICUKg - 855
EBCDICUSg - 856
ECMA-128g - 857
ECMA-CYRILLICg - 858
ECMACYRILLICg - 859
ESg - 860
ES2g - 861
EUC-CNg - 862
EUC-JISX0213g - 863
EUC-JP-MSg - 864
EUC-JPg - 865
EUC-KRg - 866
EUC-TWg - 867
EUCCNg - 868
EUCJP-MSg - 869
EUCJP-OPENg - 870
EUCJP-WINg - 871
EUCJPg - 872
EUCKRg - 873
EUCTWg - 874
FIg - 875

FRg - 876
GBg - 877
GB2312g - 878
GB13000g - 879
GB18030g - 880
GBKg - 881
GB_1988-80g - 882
GB_198880g - 883
GOST_19768-74g - 884
GOST_19768g - 885
GOST_1976874g - 886
GREEK-CCITTg - 887
GREEK7-OLDg - 888
GREEK7g - 889
GREEK7OLDg? - 890
GREEKCCITTg - 891
HUg - 892
IBM-803g - 893
IBM-856g - 894
IBM-901g - 895
IBM-902g - 896
IBM-921g - 897
IBM-922g - 898
IBM-930g - 899
IBM-932g - 900
IBM-933g - 901
IBM-935g - 902
IBM-937g - 903
IBM-939g - 904
IBM-943g - 905
IBM-1008g - 906
IBM-1025g - 907
IBM-1046g - 908
IBM-1047g - 909
IBM-1097g - 910
IBM-1112g - 911
IBM-1122g - 912
IBM-1123g - 913
IBM-1124g - 914
IBM-1129g - 915
IBM-1130g - 916
IBM-1132g - 917
IBM-1133g - 918
IBM-1137g - 919
IBM-1140g - 920
IBM-1141g - 921
IBM-1142g - 922
IBM-1143g - 923
IBM-1144g - 924
IBM-1145g - 925
IBM-1146g - 926
IBM-1147g - 927
IBM-1148g - 928
IBM-1149g - 929
IBM-1153g - 930
IBM-1154g - 931
IBM-1155g - 932
IBM-1156g - 933
IBM-1157g - 934
IBM-1158g - 935
IBM-1160g - 936
IBM-1161g - 937
IBM-1162g - 938
IBM-1163g - 939
IBM-1164g - 940
IBM-1166g - 941
IBM-1167g - 942
IBM-1364g - 943
IBM-1371g - 944
IBM-1388g - 945
IBM-1390g - 946
IBM-1399g - 947
IBM-4517g - 948
IBM-4899g - 949
IBM-4909g - 950
IBM-4971g - 951
IBM-5347g - 952
IBM-9030g - 953
IBM-9066g - 954
IBM-9448g - 955

IBM-12712g - 956
IBM-16804g - 957
IBM037g - 958
IBM038g - 959
IBM256g - 960
IBM273g - 961
IBM274g - 962
IBM275g - 963
IBM277g - 964
IBM278g - 965
IBM280g - 966
IBM281g - 967
IBM284g - 968
IBM285g - 969
IBM290g - 970
IBM297g - 971
IBM420g - 972
IBM423g - 973
IBM424g - 974
IBM437g - 975
IBM500g - 976
IBM775g - 977
IBM803g - 978
IBM813g - 979
IBM848g - 980
IBM851g - 981
IBM852g - 982
IBM855g - 983
IBM856g - 984
IBM857g - 985
IBM860g - 986
IBM861g - 987
IBM863g - 988
IBM864g - 989
IBM865g - 990
IBM866NAVg? - 991
IBM868g - 992
IBM869g - 993
IBM870g - 994
IBM871g - 995
IBM874g - 996
IBM875g - 997
IBM880g - 998
IBM891g - 999
IBM901g - 1000
IBM902g - 1001
IBM903g - 1002
IBM904g - 1003
IBM905g - 1004
IBM912g - 1005
IBM915g - 1006
IBM916g - 1007
IBM918g - 1008
IBM920g - 1009
IBM921g - 1010
IBM922g - 1011
IBM930g - 1012
IBM932g - 1013
IBM933g - 1014
IBM935g - 1015
IBM937g - 1016
IBM939g - 1017
IBM943g - 1018
IBM1004g - 1019
IBM1008g - 1020
IBM1025g - 1021
IBM1026g - 1022
IBM1046g - 1023
IBM1047g - 1024
IBM1089g - 1025
IBM1097g - 1026
IBM1112g - 1027
IBM1122g - 1028
IBM1123g - 1029
IBM1124g - 1030
IBM1129g - 1031
IBM1130g - 1032
IBM1132g - 1033
IBM1133g - 1034
IBM1137g - 1035

IBM1140g - 1036
IBM1141g - 1037
IBM1142g - 1038
IBM1143g - 1039
IBM1144g - 1040
IBM1145g - 1041
IBM1146g - 1042
IBM1147g - 1043
IBM1148g - 1044
IBM1149g - 1045
IBM1153g - 1046
IBM1154g - 1047
IBM1155g - 1048
IBM1156g - 1049
IBM1157g - 1050
IBM1158g - 1051
IBM1160g - 1052
IBM1161g - 1053
IBM1162g - 1054
IBM1163g - 1055
IBM1164g - 1056
IBM1166g - 1057
IBM1167g - 1058
IBM1364g - 1059
IBM1371g - 1060
IBM1388g - 1061
IBM1390g - 1062
IBM1399g - 1063
IBM4517g - 1064
IBM4899g - 1065
IBM4909g - 1066
IBM4971g - 1067
IBM5347g - 1068
IBM9030g - 1069
IBM9066g - 1070
IBM9448g - 1071
IBM12712g - 1072
IBM16804g - 1073
IEC_P27-1g - 1074
IEC_P271g - 1075
INIS-8g - 1076
INIS-CYRILLICg - 1077
INISg - 1078
INIS8g - 1079
INISCYRILLICg - 1080
ISIRI-3342g - 1081
ISIRI3342g - 1082
ISO-2022-CN-EXTg - 1083
ISO-2022-CNg - 1084
ISO-2022-JP-2g - 1085
ISO-2022-JP-3g - 1086
ISO-2022-JPg - 1087
ISO-2022-KRg - 1088
ISO-8859-9g - 1089
ISO-8859-10g - 1090
ISO-8859-11g - 1091
ISO-8859-16g - 1092
ISO-10646g - 1093
ISO-10646/UTF-8/ - 1094
ISO-10646/UTF8/ - 1095
ISO-IR-4g - 1096
ISO-IR-8-1g - 1097
ISO-IR-9-1g - 1098
ISO-IR-10g - 1099
ISO-IR-11g - 1100
ISO-IR-15g - 1101
ISO-IR-16g - 1102
ISO-IR-17g - 1103
ISO-IR-18g - 1104
ISO-IR-19g - 1105
ISO-IR-21g - 1106
ISO-IR-25g - 1107
ISO-IR-27g - 1108
ISO-IR-37g - 1109
ISO-IR-49g - 1110
ISO-IR-50g - 1111
ISO-IR-51g - 1112
ISO-IR-54g - 1113
ISO-IR-55g - 1114
ISO-IR-57g - 1115

ISO-IR-60g - 1116
ISO-IR-61g - 1117
ISO-IR-69g - 1118
ISO-IR-84g - 1119
ISO-IR-85g - 1120
ISO-IR-86g - 1121
ISO-IR-88g - 1122
ISO-IR-89g - 1123
ISO-IR-90g - 1124
ISO-IR-92g - 1125
ISO-IR-98g - 1126
ISO-IR-99g - 1127
ISO-IR-103g - 1128
ISO-IR-111g - 1129
ISO-IR-121g - 1130
ISO-IR-122g - 1131
ISO-IR-127g - 1132
ISO-IR-139g - 1133
ISO-IR-141g - 1134
ISO-IR-143g - 1135
ISO-IR-150g - 1136
ISO-IR-151g - 1137
ISO-IR-153g - 1138
ISO-IR-155g - 1139
ISO-IR-156g - 1140
ISO-IR-166g - 1141
ISO-IR-193g - 1142
ISO-IR-197g - 1143
ISO-IR-209g - 1144
ISO/TR_11548-1/ - 1145
ISO646-CAg - 1146
ISO646-CA2g - 1147
ISO646-CNg - 1148
ISO646-CUg - 1149
ISO646-DEg - 1150
ISO646-DKg - 1151
ISO646-ESg - 1152
ISO646-ES2g - 1153
ISO646-FIg - 1154
ISO646-FRg - 1155
ISO646-FR1g - 1156
ISO646-GBg - 1157
ISO646-HUg - 1158
ISO646-ITg - 1159
ISO646-JP-OCR-Bg - 1160
ISO646-KRg - 1161
ISO646-NOg - 1162
ISO646-NO2g - 1163
ISO646-PTg - 1164
ISO646-PT2g - 1165
ISO646-SEg - 1166
ISO646-SE2g - 1167
ISO646-YUg - 1168
ISO2022CNg? - 1169
ISO2022CNEXTg? - 1170
ISO2022JPg? - 1171
ISO2022JP2g? - 1172
ISO2022KRg? - 1173
ISO6937g - 1174
ISO8859-11g - 1175
ISO11548-1g - 1176
ISO88591g - 1177
ISO88592g - 1178
ISO88593g - 1179
ISO88594g - 1180
ISO88595g - 1181
ISO88596g - 1182
ISO88597g - 1183
ISO88598g - 1184
ISO88599g - 1185
ISO885910g - 1186
ISO885911g - 1187
ISO885913g - 1188
ISO885914g - 1189
ISO885915g - 1190
ISO885916g - 1191
ISO_2033-1983g - 1192
ISO_2033g - 1193
ISO_5427-EXTg - 1194
ISO_5427g - 1195

ISO_5427:1981g - 1196
ISO_5427EXTg - 1197
ISO_5428g - 1198
ISO_5428:1980g - 1199
ISO_6937-2g - 1200
ISO_6937-2:1983g - 1201
ISO_6937g - 1202
ISO_6937:1992g - 1203
ISO_8859-7:2003g - 1204
ISO_8859-16:2001g - 1205
ISO_9036g - 1206
ISO_10367-BOXg - 1207
ISO_10367BOXg - 1208
ISO_11548-1g - 1209
ISO_69372g - 1210
ITg - 1211
JIS_C6229-1984-Bg - 1212
JIS_C62201969ROg - 1213
JIS_C62291984Bg - 1214
JOHABg - 1215
JP-OCR-Bg - 1216
JSg - 1217
JUS_I.B1.002g - 1218
KOI-7g - 1219
KOI-8g - 1220
KOI8g - 1221
KSC5636g - 1222
L10g - 1223
LATIN-9g - 1224
LATIN-GREEK-1g - 1225
LATIN-GREEKg - 1226
LATIN10g - 1227
LATINGREEKg - 1228
LATINGREEK1g - 1229
MAC-CYRILLICg - 1230
MAC-ISg - 1231
MAC-SAMIg - 1232
MAC-UKg - 1233
MACCYRILLICg - 1234
MIKg - 1235
MS-MAC-CYRILLICg - 1236
MS932g - 1237
MS936g - 1238
MSCP949g - 1239
MSCP1361g - 1240
MSMACCYRILLICg - 1241
MSZ_7795.3g - 1242
MS_KANJIg - 1243
NAPLPSg - 1244
NATS-DANOg - 1245
NATS-SEFIg - 1246
NATSDANOg - 1247
NATSSEFIg - 1248
NC_NC0010g - 1249
NC_NC00-10g - 1250
NC_NC00-10:81g - 1251
NF_Z_62-010g - 1252
NF_Z_62-010_(1973)g - 1253
NF_Z_62-010_1973g - 1254
NF_Z_62010g - 1255
NF_Z_62010_1973g - 1256
NOg - 1257
NO2g - 1258
NS_4551-1g - 1259
NS_4551-2g - 1260
NS_45511g - 1261
NS_45512g - 1262
OS2LATIN1g? - 1263
OSF00010001g - 1264
OSF00010002g - 1265
OSF00010003g - 1266
OSF00010004g - 1267
OSF00010005g - 1268
OSF00010006g - 1269
OSF00010007g - 1270
OSF00010008g - 1271
OSF00010009g - 1272
OSF0001000Ag? - 1273
OSF00010020g - 1274
OSF00010100g - 1275

OSF00010101g - 1276
OSF00010102g - 1277
OSF00010104g - 1278
OSF00010105g - 1279
OSF00010106g - 1280
OSF00030010g - 1281
OSF0004000Ag? - 1282
OSF0005000Ag? - 1283
OSF05010001g - 1284
OSF100201A4g? - 1285
OSF100201A8g? - 1286
OSF100201B5g? - 1287
OSF100201F4g? - 1288
OSF100203B5g? - 1289
OSF1002011Cg? - 1290
OSF1002011Dg? - 1291
OSF1002035Dg? - 1292
OSF1002035Eg? - 1293
OSF1002035Fg? - 1294
OSF1002036Bg? - 1295
OSF1002037Bg? - 1296
OSF10010001g - 1297
OSF10020025g - 1298
OSF10020111g - 1299
OSF10020115g - 1300
OSF10020116g - 1301
OSF10020118g - 1302
OSF10020122g - 1303
OSF10020129g - 1304
OSF10020352g - 1305
OSF10020354g - 1306
OSF10020357g - 1307
OSF10020359g - 1308
OSF10020360g - 1309
OSF10020364g - 1310
OSF10020365g - 1311
OSF10020366g - 1312
OSF10020367g - 1313
OSF10020370g - 1314
OSF10020387g - 1315
OSF10020388g - 1316
OSF10020396g - 1317
OSF10020402g - 1318
OSF10020417g - 1319
PTg - 1320
PT2g - 1321
PT154g - 1322
RK1048g - 1323
RUSCIIg - 1324
SEg - 1325
SE2g - 1326
SEN_850200_Bg - 1327
SEN_850200_Cg - 1328
SHIFT-JISg - 1329
SHIFT_JISg - 1330
SHIFT_JISX0213g - 1331
SJIS-OPENg - 1332
SJIS-WINg - 1333
SJISg - 1334
SS636127g - 1335
STRK1048-2002g - 1336
ST_SEV_358-88g - 1337
T.61-8BITg - 1338
T.61g - 1339
T.618BITg - 1340
TS-5881g - 1341
UHCg - 1342
UJISg - 1343
UKg - 1344
UTF8g - 1345
UTF16g - 1346
UTF16BEg? - 1347
UTF16LEg? - 1348
UTF32g - 1349
UTF32BEg? - 1350
UTF32LEg? - 1351
WCHAR_Tg - 1352
WIN-SAMI-2g - 1353
WINDOWS-31Jg - 1354
WINDOWS-936g - 1355

WINSAMI2g - 1356
WS2g - 1357
YUg - 1358

Tema principal: Políticas

Alertas de correlación

Una alerta es un mensaje que indica que se ha detectado una excepción o una infracción de una regla de política.

Las alertas se desencadenan de dos formas:

- Una *alerta de correlación* la desencadena una consulta que mira hacia atrás en un periodo de tiempo especificado para determinar si se ha alcanzado el umbral de alerta. Guardium Anomaly Detection Engine ejecuta consultas de correlación regularmente. De forma predeterminada, las alertas de correlación no registran infracciones de política, pero se pueden configurar para que lo hagan.
- Las *alertas en tiempo real* las desencadenan las reglas de políticas de seguridad. El componente Guardium Inspection Engine ejecuta políticas de seguridad y recopila y analiza el tráfico de la base de datos en tiempo real.

Independientemente de cómo se desencadenan, Guardium registra todas las alertas de la misma manera: la información de las alertas se registra en la base de datos interna de Guardium. La cantidad y el tipo de información registrada depende del tipo de alerta específico. El componente Guardium Alerter, que también se ejecuta regularmente, procesa cada nueva alerta, pasando la información registrada para cada alerta a cualquier combinación de los mecanismos de notificación siguientes:

- SMTP – Servidor SMTP (correo electrónico saliente). El componente Alerter pasa los mensajes de correo electrónico estándar al servidor SMTP configurado.
- SNMP – Servidor SNMP (control e información de red). Cuando se selecciona SNMP para una notificación de alerta, el componente Alerter pasa todos los mensajes de alerta de ese tipo a la comunidad de excepciones configurada para el componente Alerter.
- Syslog - La alerta se graba en el syslog en el dispositivo Guardium (el administrador de Guardium puede configurar la grabación de mensajes de syslog en un sistema remoto).
  Nota: Tanto para SNMP como para SYSLOG, la longitud máxima de los mensajes es de 3000 caracteres. Se truncarán los mensajes de una mayor longitud.
- Personalizado - Una clase Java™ escrita por el usuario para manejar alertas. El componente Alerter pasará un mensaje de alerta y la indicación de fecha y hora a la clase de alertas personalizada. Puede haber varias clases de alertas personalizadas, y una clase de alertas personalizada puede ser una extensión de otra clase de alertas personalizadas.

Nota: La definición de las alertas y las notificaciones no están sujetas a la seguridad de nivel de datos. Entre otras razones, se debe a que las alertas no se evalúan en el contexto del usuario, la alerta puede estar relacionada con bases de datos asociadas a varios usuarios y para evitar situaciones donde al final nadie recibe la notificación.
Nota: Si hay una alerta que utiliza una consulta con 30 campos o más (incluidos contadores) la detección de anomalías fallará con un mensaje de error de `Excepción de matriz fuera de límites`. No se deberían utilizar para las alertas consultas con 30 o más columnas. Estas consultas no aparecen en la lista de consultas disponibles para alertas de umbral.

Tareas de alertas para los administradores

Los administradores de Guardium llevan a cabo las tareas siguientes:

- Personalizar la plantilla de mensajes de alerta, utilizando el perfil global.
- Configurar e iniciar el componente Alerter, que entrega mensajes a servidores SMTP, SNMP, Syslog o a clases de alerta personalizadas.
- Iniciar y detener el motor de detección de anomalías, que ejecuta las alertas de correlación de acuerdo con las planificaciones definidas.
- Subir las clases de alertas personalizadas al sistema Guardium.

Tareas de alertas para los usuarios

Los usuarios de Guardium (y los administradores) pueden realizar estas tareas de alertas de correlación:

- Definir consultas que se utilizarán para las alertas de correlación
- Definir alertas de correlación
- Escribir clases de alertas personalizadas

Acerca de las consultas de las alertas de correlación

Una alerta de correlación se basa en una consulta de cualquiera de los dominios de creación de informes. Antes de definir una alerta, hay que definir la consulta. Para que esté disponible para ser utilizada por una alerta de correlación, la consulta debe contener al menos un campo de fecha.

Creación de una alerta de correlación

1. Pulse Proteger > Detección de intrusión en base de datos > Creador de alertas para abrir el Buscador de alertas.
2. Pulse Nueva en el panel del Buscador de alertas para visualizar el panel Añadir alerta.
3. Especifique un nombre exclusivo para la alerta en el recuadro Nombre. No incluya caracteres de apóstrofo en el nombre de alerta.
4. Especifique una frase breve que describa la alerta en el recuadro Descripción.
5. Especifique una categoría opcional en el recuadro Categoría.
6. Especifique una clasificación opcional en el recuadro Clasificación.
7. En la Acción recomendada, el usuario puede añadir texto libre como acción recomendada para la alerta específica.
8. Al igual que en las alertas en tiempo real, el usuario puede elegir una plantilla para el mensaje que se envía en caso de que se active la alerta de umbral. La plantilla utiliza una lista predefinida de variables que se sustituyen por el valor apropiado para la alerta específica. La lista de variables y una plantilla predeterminada se detallan en la sección de Plantillas con nombre del tema de ayuda del Perfil global.
9. Seleccione un nivel de gravedad de la lista de Gravedad. Para una alerta de correo electrónico, un valor de gravedad ALTA da lugar a que el correo electrónico se marque como urgente.
10. Especifique el número de minutos entre ejecuciones de la consulta en el campo Frecuencia de ejecución.
11. Marque el recuadro Activar para activar la alerta, o desmarque el recuadro para guardar la definición de alerta sin iniciar su ejecución (se podrá activar más tarde) En un entorno de Gestor central (CM), la alerta se activará (o se detendrá) en todas las unidades gestionadas cuando este recuadro esté marcado (desmarcado). Para inhabilitar la alerta en un dispositivo específico en un entorno de Gestor central, utilice el panel Detección de anomalías de la Consola del administrador.
12. Marque el recuadro Registrar infracción de política para registrar una infracción de política cuando se desencadene esta alerta. De forma predeterminada, las alertas de correlación sólo se registran en el dominio de Seguimiento de alertas. Marcando este recuadro, las alertas de correlación y las alertas en tiempo real

(emitidas por la política de seguridad de acceso a datos) se pueden visualizar conjuntamente, en el dominio de Infracciones de política.

13. En la lista de Consulta del panel Definición de alerta, seleccione la consulta que desea ejecutar para esta alerta. La lista de consultas visualizada incluirá todas las consultas definidas que:
    - Contienen al menos un campo de fecha (indicación de fecha y hora) - el campo de indicación de fecha y hora es obligatorio
    - Contienen un campo de recuento - un campo de recuento es obligatorio
    - Sean accesibles por su cuenta de usuario de Guardium

    Sugerencias para la resolución de problemas
    - Si se ha creado una consulta personalizada en un Creador de consultas de Creación de informes y no aparece en la lista de Consulta, asegúrese de que la consulta personalizada tiene una indicación de fecha y hora (campo fecha).
    - Si después de seleccionar una consulta de la lista de Consulta en el panel Definición de alerta de la pantalla Añadir alerta no es posible editar la consulta (icono Editar), vaya al Creador de consultas (Herramientas > Creación de informes) para editar la consulta.
14. Si la consulta seleccionada contiene parámetros de tiempo de ejecución, se mostrará un panel de Parámetros de consulta en el panel Definición de alerta. Proporcione los valores de parámetro según corresponda a la aplicación.
15. En el recuadro Intervalo de acumulación, especifique el intervalo de tiempo (en minutos) que la consulta debe examinar el repositorio de auditoría contando hacia atrás desde el instante actual (por ejemplo, especifique 10 para examinar los últimos 10 minutos de datos).
    Nota: Las alertas que se ejecutan en los agregadores se basan sólo en los datos con el periodo de fusión definido.
16. Marque el recuadro Registrar resultado de consulta completos para registrar un informe completo con la alerta.
17. Si la consulta seleccionada contiene una o más columnas de datos numéricos, seleccione una de esas columnas para utilizarla para la prueba. De forma predeterminada, será el último elemento de la lista, es decir, la última columna para la consulta, que siempre es el recuento de apariciones agregadas en dicha fila.
18. En el panel Umbral de alerta defina de la siguiente manera el umbral en el que debe generarse una alerta de correlación:
    - En el campo Umbral, especifique un valor de umbral que se aplicará tal como se describe en el resto de los campos del panel.
    - Desde Alerta cuando se liste el valor, seleccione un operador que indique cómo debe relacionarse el valor de informe con el umbral para producir una alerta (mayor que, mayor que o igual a, menor que, etc.).
    - Seleccione por informe si el valor de umbral se aplica a un total de informe, o seleccione por línea si el umbral se aplica a una única línea del informe (siendo el informe la salida de la consulta seleccionada, inspeccionando en el pasado desde el instante actual de acuerdo al tiempo de acumulación especificado).

      Si no hay datos durante el Intervalo de acumulación especificado:

      Si el umbral es por informe, el valor para ese intervalo es 0 (cero), y se generará una alerta si se cumple la condición de umbral (por ejemplo, si la condición especificada es "Alerta cuando el valor es < 1").

      Si el umbral es por línea, no se generará ninguna alerta, independientemente de la condición especificada (esto se deberá a que no hay líneas de salida).

    - Seleccione Como límite absoluto para indicar que el umbral especificado es un valor absoluto o seleccione Como cambio de porcentaje dentro del periodo para indicar que el umbral representa un porcentaje de cambio dentro del periodo de tiempo identificado en los campos Desde y Hasta.

      Si se selecciona la opción Como porcentaje de cambio dentro del periodo, utilice los controles del selector de fechas para seleccionar las fechas Desde y Hasta.

      Si se selecciona Como cambio de porcentaje para el mismo "Periodo de acumulación" en un tiempo relativo, se especificará una fecha relativa y la alerta ejecutará la consulta para el periodo actual y para el periodo relativo (utilizando el mismo intervalo) y comprobará los valores como un porcentaje del valor del periodo base.
      Nota: Si se utiliza un periodo relativo, cada vez que se comprueba la alerta, la consulta se ejecutará dos veces, una para el periodo actual y otra vez para el periodo relativo.
19. Indique en el recuadro Frecuencia de notificación con qué frecuencia (en minutos) se debe notificar a los receptores de las alertas cuando se ha satisfecho la condición de alerta.
20. Pulse Guardar para guardar la definición de alerta.
    Nota: No se puede asignar receptores o roles, ni especificar comentarios hasta que la definición se haya guardado.
21. En el panel Receptores de alertas, puede designar una o más personas o grupos para ser notificados cuando se satisfaga esta condición de alerta. Para añadir un receptor, pulse el botón Añadir receptor para abrir el panel de selección de Añadir receptor.
    Nota: Si el receptor de una alerta es el usuario administrador, es necesario que tenga asignado un correo electrónico para que se active la alerta.
    Nota: Un receptor adicional para las alertas de umbral es el propietario o propietarios de la base de datos. Si la consulta asociada con la alerta contiene la dirección IP del servidor y el nombre de servicio y si la alerta se evalúa por filas, el receptor puede ser el Propietario. La notificación de la alerta debe tener: Tipo de notificación de alerta: Correo, ID de usuario de alerta: 0, Destino de alerta: Propietario. Consulte las Acciones de alerta en Políticas para receptores adicionales para alertas en tiempo real.
22. Opcionalmente, pulse Roles para asignar roles a la alerta.
23. Opcionalmente, pulse Comentarios para añadir comentarios a la definición.
24. Pulse Aplicar y, a continuación, Terminado cuando haya terminado.

Modificación de una alerta de correlación

1. Pulse Proteger > Detección de intrusión en base de datos > Creador de alertas para abrir el Buscador de alertas.
2. Seleccione la alerta de correlación que desea modificar, en el panel Buscador de alertas.
3. Pulse Modificar para abrir el panel Modificar alerta.
4. Consulte el tema de Creación de una alerta de correlación para realizar cambios a la definición de la alerta.
5. Pulse Guardar.

Eliminación de una alerta de correlación

1. Pulse Proteger > Detección de intrusión en base de datos > Creador de alertas para abrir el Buscador de alertas.
2. Seleccione la alerta de correlación que desea eliminar en el panel Buscador de alertas.
3. Pulse el botón Suprimir. Se le solicitará que confirme la acción.

Tema principal: Protección

Señalización de sucesos a través de las alertas de correlación

Desencadenar una alerta de correlación si hay más de quince errores de SQL en las últimas tres horas para un usuario individual cualquiera de la aplicación.

Acerca de esta tarea

Las alertas de correlación permiten informar de los sucesos acumulados a lo largo del tiempo. Las aplicaciones no suelen tener errores de SQL. Un aumento en los errores SQL en una aplicación podría ser un aviso de un posible intento de inyección de SQL. Consulte los temas de ayuda en línea, Alertas de correlación y Consultas para obtener más información.

Requisitos previos

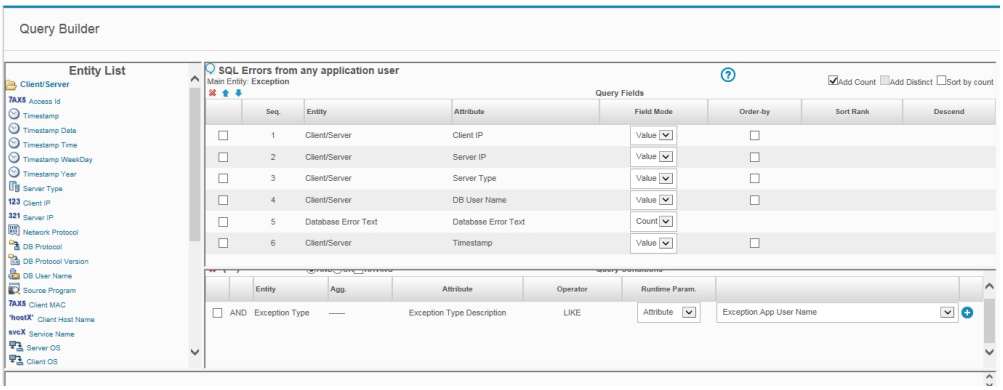
- Configurar el servidor de correo electrónico (SMTP) (Configuración > Herramientas y vistas > Alertador)
- Después de configurar completamente la alerta de correlación, asegúrese de que está activa y en ejecución (Configuración > Vistas y vistas > Detección de anomalías).

Una alerta es un mensaje que indica que se ha detectado una excepción (alerta de correlación) o una infracción de una regla de política (alerta en tiempo real).

Una alerta de correlación la desencadena una consulta que mira hacia atrás en un periodo de tiempo especificado para determinar si se ha alcanzado un umbral de alerta.

Visión general de los pasos de la alerta de correlación

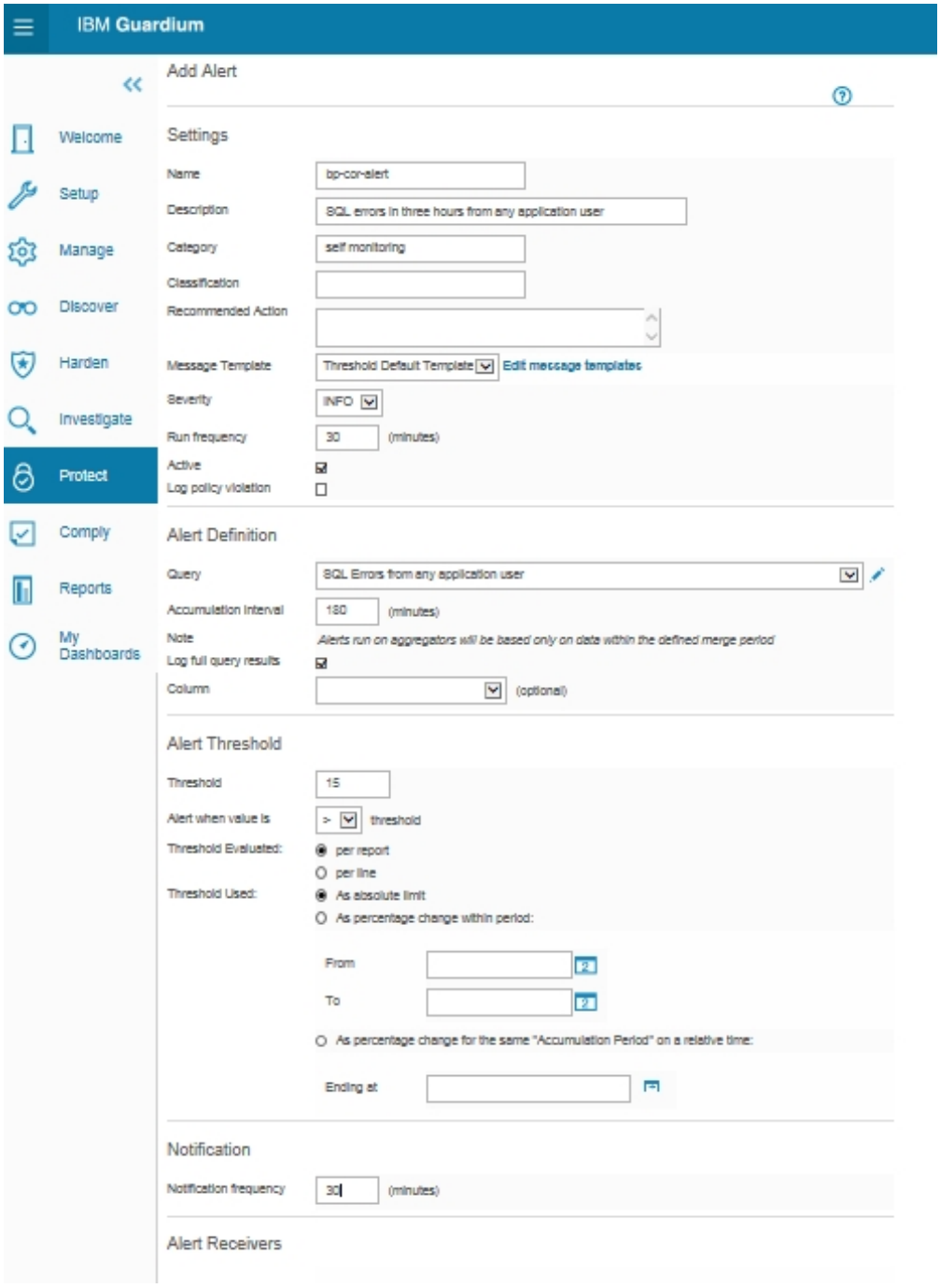
1. Cree una consulta personalizada a partir del Seguimiento de excepciones con un campo de Errores de SQL (con un recuento) y una condición de usuarios de la aplicación. Para poder utilizar esta consulta personalizada en el Creador de alertas, es necesario un campo de fecha (indicación de fecha y hora).
2. Pulse Proteger > Detección de intrusión en base de datos > Creador de alertas para abrir el Buscador de alertas.
3. Pulse en Nuevo. Complete los campos según las instrucciones que se proporcionan en la pantalla de menú del Creador de alertas.
4. Añada un receptor.



Dominio de excepciones, Consulta de errores de SQL

Procedimiento

1. Seguimiento de excepciones - Abrir el Buscador de consultas
   - Usuarios: Seleccionar herramientas > Creación de informes y, a continuación, seleccione únicamente el dominio Excepciones.
2. Abra las opciones desplegables para la consulta. Seleccione Errores de SQL. Con esta acción abrirá una ventana de configuración con el título principal de Errores de SQL.
3. Clone esta selección, escribiendo un nombre exclusivo en el recuadro de texto para la consulta. No incluya caracteres de apóstrofo en el nombre de consulta.
4. En la consulta personalizada, bajo los campos de Consulta, desde la lista de entidades de Cliente/Servidor, añada un campo de fecha (indicación de fecha y hora) y cambie campo del texto de error de la base de datos a la modalidad de campo de recuento. Bajo las condiciones de la consulte, cambie los parámetros de tiempo de ejecución de los tipos de excepción a atributo y elija Excecpión.Nombre usuario aplicación.
5. Pulse Guardar. Esta consulta personalizada para errores de SQL de cualquier usuario de la aplicación está ahora disponible para su uso en el Creador de alertas.



Pantalla del menú del Creador de alertas

6. Creador de alertas - Cree una alerta de correlación
7. Pulse Proteger > Detección de intrusión en base de datos > Creador de alertas para abrir el Buscador de alertas.
8. Pulse el botón Nueva en el panel del Buscador de alertas para visualizar el panel Añadir alerta.
9. Especifique un nombre exclusivo para la alerta en el recuadro Nombre. No incluya caracteres de apóstrofo en el nombre de alerta.
10. Especifique una frase breve que describa la alerta en el recuadro Descripción.
11. Especifique una categoría opcional en el recuadro Categoría. En este caso, se ha utilizado la Autosupervisión.
12. Especifique una clasificación opcional en el recuadro Clasificación.
13. Seleccione un nivel de gravedad de la lista de Gravedad. Para una alerta de correo electrónico, un valor de gravedad ALTA da lugar a que el correo electrónico se marque como urgente.
14. Especifique el número de minutos entre ejecuciones de la consulta en el campo Frecuencia de ejecución.
15. Marque el recuadro Activar para activar la alerta.
16. Marque el recuadro Registrar infracción de política para registrar una infracción de política cuando se desencadene esta alerta. De forma predeterminada, las alertas de correlación sólo se registran en el dominio de Seguimiento de alertas. Marcando este recuadro, las alertas de correlación y las alertas en tiempo real (emitidas por la política de seguridad de acceso a datos) se pueden visualizar conjuntamente, en el dominio de Infracciones de política.
17. En la lista de Consulta del panel Definición de alerta, seleccione la consulta que desea ejecutar para esta alerta. La lista de consultas visualizada incluirá todas las consultas definidas que:
    - Contienen al menos un campo de fecha (indicación de fecha y hora) - el campo de indicación de fecha y hora es obligatorio
    - Contienen un campo de recuento - un campo de recuento es obligatorio
    - Sean accesibles por su cuenta de usuario de Guardium

Sugerencias para la resolución de problemas: Si se ha creado una consulta personalizada en un Creador de consultas de Creación de informes y no aparece en la lista de Consulta, asegúrese de que la consulta personalizada tiene una indicación de fecha y hora (campo fecha).

Sugerencias para la resolución de problemas: Si después de seleccionar una consulta de la lista de Consulta en el panel Definición de alerta de la pantalla Añadir alerta no es posible editar la consulta (icono Editar), vaya al Creador de consultas (Herramientas > Creación de informes) para editar la consulta.

18. Si la consulta seleccionada contiene parámetros de tiempo de ejecución, se mostrará un panel de Parámetros de consulta en el panel Definición de alerta. Proporcione los valores de parámetro según corresponda a la aplicación.
19. En el recuadro Intervalo de acumulación, especifique el intervalo de tiempo (en minutos) que la consulta debe examinar el repositorio de auditoría contando hacia atrás desde el instante actual (por ejemplo, especifique 10 para examinar los últimos 10 minutos de datos).
20. Marque el recuadro Registrar resultado de consulta completos para registrar un informe completo con la alerta.
21. Si la consulta seleccionada contiene una o más columnas de datos numéricos, seleccione una de esas columnas para utilizarla para la prueba. De forma predeterminada, será el último elemento de la lista, es decir, la última columna para la consulta, que siempre es el recuento de apariciones agregadas en dicha fila.
22. En el panel Umbral de alerta defina de la siguiente manera el umbral en el que debe generarse una alerta de correlación:
    - En el campo Umbral, especifique un valor de umbral que se aplicará tal como se describe en el resto de los campos del panel.
    - Desde Alerta cuando se liste el valor, seleccione un operador que indique cómo debe relacionarse el valor de informe con el umbral para producir una alerta (mayor que, mayor que o igual a, menor que, etc.).
    - Seleccione por informe si el valor de umbral se aplica a un total de un informe.

    Si no hay datos durante el Intervalo de acumulación especificado: Si el umbral es por informe, el valor para ese intervalo es 0 (cero), y se generará una alerta si se cumple la condición de umbral (por ejemplo, si la condición especificada es "Alerta cuando el valor es < 1").

23. Indique en el recuadro Frecuencia de notificación con qué frecuencia (en minutos) se debe notificar a los receptores de las alertas cuando se ha satisfecho la condición de alerta.
24. Pulse el botón Aplicar para guardar la definición de alerta.
    Nota: No se puede asignar receptores o roles, ni especificar comentarios hasta que la definición se haya guardado.
25. En el panel Receptores de alertas, puede designar una o más personas o grupos para ser notificados cuando se satisfaga esta condición de alerta. Para añadir un receptor, pulse el botón Añadir receptor para abrir el panel de selección de Añadir receptor. Para obtener información sobre la adición de receptores, consulte las notificaciones.
26. Opcionalmente, pulse Roles para asignar roles a la alerta. Consulte Roles de seguridad.
27. Opcionalmente, pulse Comentarios para añadir comentarios a la definición.
28. Pulse el botón Aplicar y, a continuación, el botón Hecho cuando haya terminado.

    Si hay más de quince errores SQL en las últimas tres horas para cualquier usuario de la aplicación, se enviará una alerta al receptor designado.

Tema principal: Protección

Gestión de incidencias

La aplicación IIM (Integrated Incident Management) proporciona una interfaz de usuario empresarial con automatización del flujo de trabajo para el seguimiento y resolución de incidencias de seguridad de base de datos.

Simplifica la gestión de incidencias al permitir a los administradores agrupar una serie de infracciones de política relacionadas en un única incidencia para asignarla a personas específicas. De esta forma se reduce el número de infracciones de política independientes que los equipos de supervisión deben revisar.

Los procesos de generación de incidencias pueden definirse y planificarse para que lean el registro de infracciones de política y generen nuevas incidencias. Desde un proceso de generación de incidencias, cada incidencia seleccionada es:

- Asignada a un número de incidencia exclusivo
- Asignada a un usuario
- Asignada a un código de gravedad
- Asignada a una categoría

Además, las infracciones de política se pueden asignar manualmente (por los usuarios autorizados) a nuevas incidencias o a incidencias existentes desde el informe de Infracciones de política / Gestión de incidencias.

Una vez que se ha generado una incidencia, los administradores y otros usuarios trabajarán con las incidencias desde el separador Gestión de incidencias, que se incluye tanto en el portal de usuario como en el portal del administrador. Desde allí, se pueden realizar todas las demás tareas (asignar incidencias, enviar notificaciones, asignar estados, etc.).

Se puede acceder a las funciones de Gestión de incidencias desde los menús desplegables de los informes de Gestión de incidencias. Cada usuario tendrá un subconjunto de informes o funciones disponibles, en función de los roles de seguridad asignados a la cuenta de usuario.

Puede crear sus propias copias de los informes de Gestión de incidencias, sin embargo, estas copias no tendrán todas las funcionalidades disponibles en los informes preconfigurados en el separador Gestión de incidencias. Para asignar incidencias, códigos de gravedad, etcétera, utilice los informes del separador Gestión de incidencias.

Definición de un proceso de generación de incidencias

Un proceso de generación de incidencias ejecuta una consulta con relación al registro de infracciones de políticas y genera incidencias basadas en dicha consulta. De forma predeterminada, la definición y la planificación de los procesos de generación de incidencias está restringida a los usuarios con el rol de administrador.

1. Pulse Cumplir > Herramientas y vistas > Generación de incidencias para abrir Procesos de generación de incidencias.
2. Pulse Añadir proceso para abrir el panel Editar proceso de generación de incidencias.
3. Seleccione una consulta en la lista de Consultas. Existen varias restricciones que se aplican a las consultas utilizadas en un proceso de generación de incidencias. Le sugerimos que abra la consulta en el Creador de consultas para verificar que cumple los criterios siguientes:
    - La consulta debe ser del dominio de Infracciones de política.
    - La consulta debe tener seleccionado el recuadro de selección Añadir recuento. Consulte Consultas para obtener más información.
    - La entidad principal de la consulta debe ser la entidad Infracción de regla de política.
    - Los campos de la consulta no deben incluir una serie SQL (desde la entidad SQL o desde el atributo Serie SQL completa de la entidad Infracción de regla de política).
4. Seleccione una Gravedad para la incidencia (el valor predeterminado es Información).
5. Opcionalmente, especifique una Categoría para la incidencia (el valor predeterminado es ninguna).

6. Opcionalmente, especifique un Umbral para la generación de la incidencia. El valor predeterminado es uno, lo que significa que cada fila devuelta por la consulta generará una incidencia.
7. En la lista Asignar a usuario, seleccione el usuario a quien se le asignará la incidencia.
8. Especifique las fechas Desde y Hasta para la consulta. Para una consulta planificada, utilice fechas relativas (por ejemplo: NOW -1 DAY y NOW).
9. Pulse Guardar para guardar la definición del proceso. No es posible ejecutar ni planificar el proceso hasta que se haya guardado.
10. Para ejecutar la consulta ahora, pulse Ejecutar una vez ahora.
11. Para planificar la consulta, pulse Modificar planificación para abrir el programa de utilidad de planificación de propósito general.

Asignación/Reasignación de incidencias

1. Efectúe una doble pulsación en la infracción de política que se va a asignar o reasignar, en uno de los informes de Gestión de incidencias.
2. Seleccione Asignar/Reasignar a incidencia desde el menú profundizable. Cuando se selecciona, este menú se sustituirá por un nuevo que contiene una lista de incidencias abiertas (por ejemplo, Asignar la incidencia número 123), y una opción adicional: Asignar a una nueva incidencia.
3. Seleccione una incidencia para asignar a esta infracción, o seleccione Asignar a una nueva incidencia para asignar esta infracción de política al siguiente número de incidencia disponible (se numeran de forma secuencial).

   Se visualiza un mensaje cuando se completa el cambio y se renovará el panel Gestión de incidencias. Si se crea una nueva incidencia, aparecerá en primer lugar en el informe de Incidencias abiertas.

Asignación a un usuario

1. Efectúe una doble pulsación en la incidencia para asignarla a otro usuario, en uno de los informes de Gestión de incidencias.
2. Seleccione Asignar a usuario en el menú profundizable. Cuando se selecciona, este menú será reemplazado con un nuevo menú que contendrá una lista de usuarios, y una opción adicional: Anular la asignación.
3. Seleccione un usuario o seleccione Anular la asignación para eliminar el usuario actualmente asignado. Cuando se asigna un usuario, la Descripción de estado será Asignada, y cuando no lo esté la Descripción de estado será Abierta.

   Se visualiza un mensaje cuando se completa el cambio y se renovará el panel Gestión de incidencias.

Cambio de gravedad

1. Efectúe una doble pulsación en la incidencia cuya gravedad desea cambiar, en uno de los informes de Gestión de incidencias.
2. Seleccione Cambiar gravedad en el menú profundizable. Cuando se selecciona, este menú será reemplazado con un nuevo menú que contendrá una lista códigos de gravedad: Información, Baja, Media y Alta.
3. Seleccione el nuevo código de gravedad.

   Se visualiza un mensaje cuando se completa el cambio y se renovará el panel Gestión de incidencias.

Notificación

1. Efectúe una doble pulsación en la incidencia que se debe notificar a un usuario, en uno de los informes de Gestión de incidencias.
2. Seleccione Notificar en el menú profundizable. Cuando se selecciona, este menú será reemplazado con un nuevo menú que contendrá una lista de usuarios.
3. Seleccione un usuario.

   Se visualiza un mensaje cuando el usuario ha sido notificado.

Cambio de estado

1. Efectúe una doble pulsación en la incidencia cuyo estado desea cambiar, en uno de los informes de Gestión de incidencias.
2. Seleccione Cambiar estado en el menú profundizable. Cuando se selecciona, este menú será reemplazado con un nuevo menú que contendrá una lista de códigos de estado:
   - ASIGNADA - No es posible añadir infracciones de política adicionales una vez que una incidencia tiene este estado. Para añadir infracciones de política, vuelva a cambiar el estado de la incidencia a Abierta, añada las infracciones y, a continuación, vuelva a cambiar el estado a Asignado.
   - CERRADA - Una vez que la incidencia se ha marcado como Cerrada, no se puede modificar y deja de aparece en la lista.
   - ABIERTA - Este es el estado inicial de un nueva incidencia.
3. Seleccione el nuevo código de estado.

   Se visualiza un mensaje cuando se completa el cambio y se renovará el panel Gestión de incidencias.

Adición de comentarios

1. Efectúe una doble pulsación en la incidencia a la que desea añadir comentarios, en uno de los informes de Gestión de incidencias.
2. Seleccione Comentarios en el menú profundizable para abrir la ventana Comentario de usuario. Para obtener instrucciones sobre cómo añadir comentarios, consulte Comentarios.

Tema principal: Protección

Gestión de la revisión de las incidencias de seguridad de varias bases de datos

Gestión de incidencias - Seguimiento y resolución de incidencias de seguridad de base de datos.

Acerca de esta tarea

Los administradores pueden agrupar una grupo de infracciones de política relacionadas en una única incidencia y asignarla a personas específicas. De esta forma se reduce el número de infracciones de política independientes que los equipos de supervisión deben revisar.

Requisitos previos

- Crear una política (Véase Políticas).
- Iniciar los motores de inspección (Consulte Configuración del motor de inspección).

Una política de seguridad contiene un conjunto ordenado de reglas que se deben aplicar al tráfico observado entre servidores y clientes de base de datos.

Se registra una infracción de política cada vez que se desencadena una regla. Las infracciones de política se pueden asignar a incidencias, ya sea automáticamente por un proceso o manualmente por parte de usuarios autorizados (consulte Gestión de incidencias).

Resumen de pasos

1. Pulse Cumplir > Herramientas y vistas > Generación de incidencias para abrir Procesos de generación de incidencias.
2. Edite el proceso de generación de incidencias (consulta, gravedad, umbral, planificación).
3. Vaya al separador Gestión de incidencias para los informes.

Gestión de incidencias

La aplicación IIM (Integrated Incident Management) proporciona una interfaz de usuario empresarial con automatización del flujo de trabajo para el seguimiento y resolución de incidencias de seguridad de base de datos.

Los procesos de generación de incidencias pueden definirse y planificarse para que lean el registro de infracciones de política y generen nuevas incidencias. Desde un proceso de generación de incidencias, cada incidencia seleccionada es:

- Asignada a un número de incidencia exclusivo.
- Asignada a un usuario.
- Asignada a un código de gravedad.
- Asignada a una categoría.

Además, las infracciones de política se pueden asignar manualmente (por los usuarios autorizados) a nuevas incidencias o a incidencias existentes desde el informe de Infracciones de política / Gestión de incidencias.

Una vez que se ha generado una incidencia, los administradores y otros usuarios trabajarán con las incidencias desde el separador Gestión de incidencias, que se incluye tanto en el portal de usuario como en el portal del administrador. Desde allí, se pueden realizar todas las demás tareas (asignar incidencias, enviar notificaciones, asignar estados, etc.).

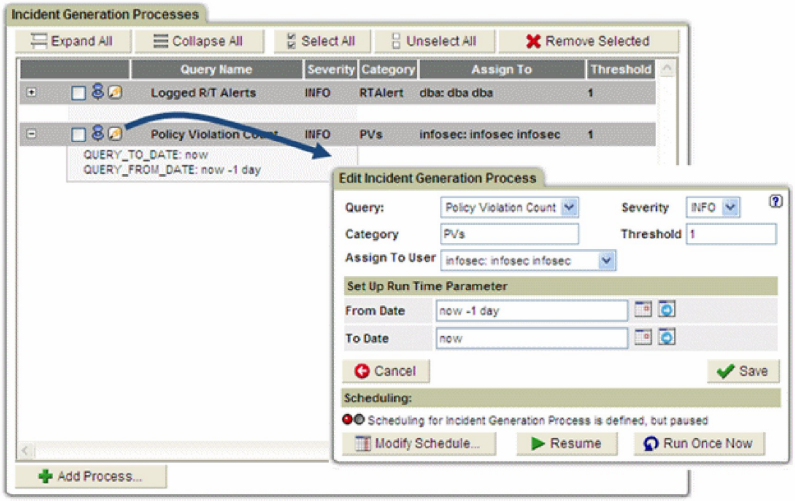
Se puede acceder a las funciones de Gestión de incidencias desde los menús desplegables de los informes de Gestión de incidencias. Cada usuario tendrá un subconjunto de informes o funciones disponibles, en función de los roles de seguridad asignados a la cuenta de usuario.

Definición de un proceso de generación de incidencias

Un proceso de generación de incidencias ejecuta una consulta con relación al registro de infracciones de políticas y genera incidencias basadas en dicha consulta. De forma predeterminada, la definición y la planificación de los procesos de generación de incidencias está restringida a los usuarios con el rol de administrador.

Procedimiento

1. Pulse Cumplir > Herramientas y vistas > Generación de incidencias para abrir Procesos de generación de incidencias.
2. Pulse el botón Añadir proceso para abrir el panel Editar proceso de generación de incidencias.
3. Seleccione una consulta en la lista de Consultas. Existen varias restricciones que se aplican a las consultas utilizadas en un proceso de generación de incidencias. Abra la consulta en el Creador de consultas para verificar que cumple los criterios siguientes:
   - La consulta debe ser del dominio de Infracciones de política.
   - La consulta debe tener marcado el recuadro de selección Añadir contador. Consulte Visión general del Creador de consultas para obtener más información.
   - La entidad principal de la consulta debe ser la entidad Infracción de regla de política.
   - Los campos de la consulta no deben incluir una serie SQL (desde la entidad SQL o desde el atributo Serie SQL completa de la entidad Infracción de regla de política).
4. Seleccione una Gravedad para la incidencia (el valor predeterminado es Información).
5. Opcionalmente, especifique una Categoría para la incidencia (el valor predeterminado es ninguna).
6. Opcionalmente, especifique un Umbral para la generación de la incidencia. El valor predeterminado es uno, lo que significa que cada "fila" devuelta por la consulta generará una incidencia.
7. En la lista Asignar a usuario, seleccione el usuario a quien se le asignará la incidencia.
8. Especifique las fechas Desde y Hasta para la consulta. Para una consulta planificada, utilice fechas relativas (por ejemplo: NOW -1 DAY y NOW).
9. Pulse Guardar para guardar la definición del proceso. No es posible ejecutar ni planificar el proceso hasta que se haya guardado.
10. Para ejecutar la consulta ahora, pulse Ejecutar una vez ahora.
11. Para planificar la consulta, pulse Modificar planificación para abrir el programa de utilidad de planificación. Para obtener instrucciones sobre cómo utilizar el planificador, consulte Planificación.

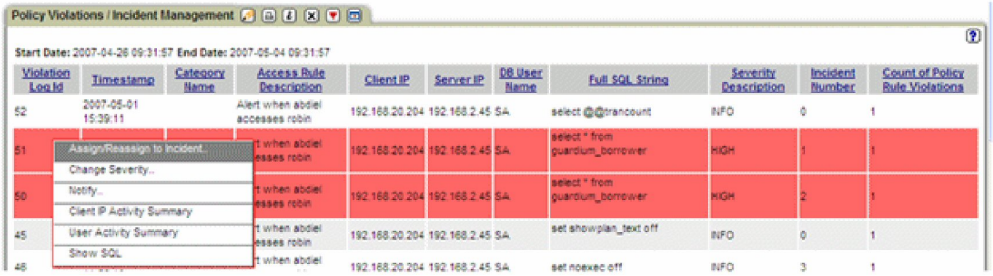


12. Asignar/Reasignar a incidencia - Efectúe una doble pulsación en la infracción de política que se va a asignar o reasignar, en uno de los informes de Gestión de incidencias.
13. Seleccione Asignar/Reasignar a incidencia desde el menú profundizable. Cuando se selecciona, este menú se sustituirá por un nuevo que contiene una lista de incidencias abiertas (por ejemplo, Asignar la incidencia número 123), y una opción adicional: Asignar a una nueva incidencia.
14. Seleccione una incidencia para asignar a esta infracción, o seleccione Asignar a una nueva incidencia para asignar esta infracción de política al siguiente número de incidencia disponible (se numeran de forma secuencial).

    Se visualiza un mensaje cuando se completa el cambio y se renovará el panel Gestión de incidencias. Si se crea una nueva incidencia, aparecerá en primer lugar en el informe de Incidencias abiertas.

    Desde el informe de Infracciones de política / Gestión de incidencias, los usuarios pueden:

    - Asignar/Reasignar a incidencia (crear una incidencia a partir de esta infracción de política).
    - Cambiar la gravedad de la incidencia.
    - Notificar a uno o más usuarios sobre la incidencia.
    - Ver informes de Actividad de IP de cliente, Actividad de usuario o SQL de la incidencia.



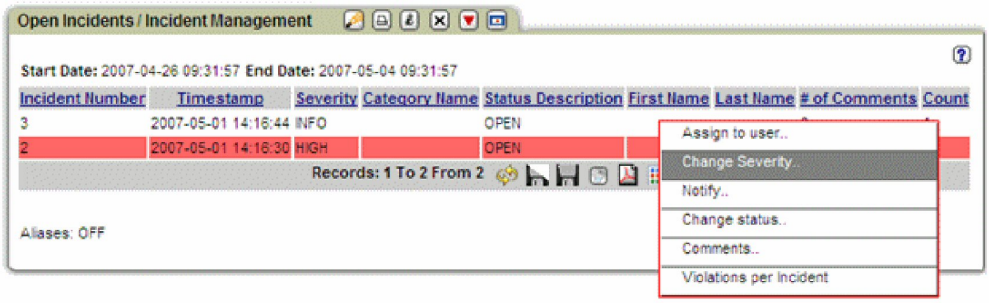
15. Asignar a usuario - Efectúe una doble pulsación en la incidencia para asignarla a otro usuario, en uno de los informes de Gestión de incidencias.
16. Seleccione Asignar a usuario en el menú profundizable. Cuando se selecciona, este menú será reemplazado con un nuevo menú que contendrá una lista de usuarios, y una opción adicional: Anular la asignación.
17. Seleccione un usuario o seleccione Anular la asignación para eliminar el usuario actualmente asignado. Cuando se asigna un usuario, la Descripción de estado será Asignada, y cuando no lo esté la Descripción de estado será Abierta.

    Se visualiza un mensaje cuando se completa el cambio y se renovará el panel Gestión de incidencias.

18. Cambiar la gravedad - Efectúe una doble pulsación en la incidencia cuya gravedad desea cambiar, en uno de los informes de Gestión de incidencias.
19. Seleccione Cambiar gravedad en el menú profundizable. Cuando se selecciona, este menú será reemplazado con un nuevo menú que contendrá una lista códigos de gravedad: Información, Baja, Media y Alta.
20. Seleccione el código de gravedad deseado.

    Se visualiza un mensaje cuando se completa el cambio y se renovará el panel Gestión de incidencias.

    Una vez que una infracción de política se ha asignado a una incidencia, la incidencia se visualiza en el informe Incidencias abiertas. Desde el informe Incidencias abiertas, los usuarios pueden realizar las acciones que se muestran:



21. Notificar - Efectúe una doble pulsación en la incidencia que se debe notificar a un usuario, en uno de los informes de Gestión de incidencias.
22. Seleccione Notificar en el menú profundizable. Cuando se selecciona, este menú será reemplazado con un nuevo menú que contendrá una lista de usuarios.
23. Seleccione un usuario.

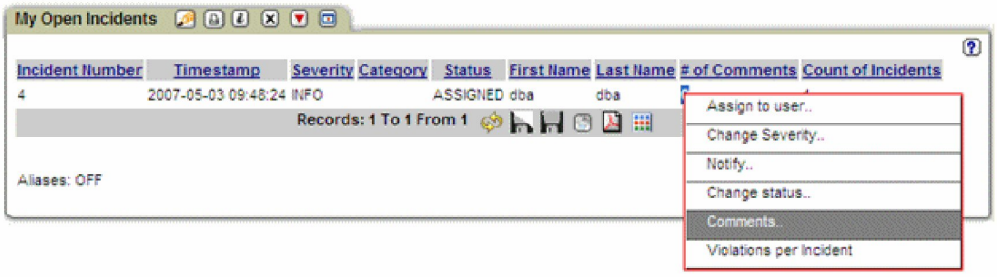
    Se visualizará un mensaje cuando el usuario reciba la notificación.

24. Cambiar estado - Efectúe una doble pulsación en la incidencia cuyo estado desea cambiar, en uno de los informes de Gestión de incidencias.
25. Seleccione Cambiar estado en el menú profundizable. Cuando se selecciona, este menú será reemplazado con un nuevo menú que contendrá una lista de códigos de estado:
    - ASIGNADA - No es posible añadir infracciones de política adicionales una vez que una incidencia tiene este estado. Para añadir infracciones de política, vuelva a cambiar el estado de la incidencia a Abierta, añada las infracciones y, a continuación, vuelva a cambiar el estado a Asignado.
    - CERRADA - Una vez que la incidencia se ha marcado como Cerrada, no se puede modificar y deja de aparece en la lista.
    - ABIERTA - Este es el estado inicial de un nueva incidencia.
26. Seleccione el código de estado deseado.

    Se visualiza un mensaje cuando se completa el cambio y se renovará el panel Gestión de incidencias.

27. Añadir comentario - Efectúe una doble pulsación en la incidencia a la que desea añadir comentarios, en uno de los informes de Gestión de incidencias.
28. Seleccione Comentarios en el menú profundizable para abrir la ventana Comentario de usuario. Para obtener instrucciones sobre cómo añadir comentarios, consulte Comentarios.

    Cada portal de usuario muestra un informe de Mis incidencias abiertas para dicho usuario. Desde el informe Mis incidencias abiertas, los usuarios pueden realizar las acciones que se muestran:



Tema principal: Protección

Reescritura de consultas

La funcionalidad de reescritura de consultas proporciona un control de acceso preciso para las bases de datos mediante la interceptación de consultas de bases de datos y su reescritura en función de los criterios definidos en las políticas de seguridad.

La modificación de las consultas se produce de forma transparente y sobre la marcha, de forma que un usuario que emita consultas recibirá de forma transparente resultados basados en sentencias de SQL reescritas.

La funcionalidad de reescritura de consultas se implementa a través de una combinación de definiciones de reescritura de consultas que indican cómo se deben cambiar o aumentar las consultas y un contexto de tiempo de ejecución que indica las circunstancias específicas en las que se deben aplicar las definiciones de reescritura de consultas.

La reescritura de consultas de base de datos al instante sobre la marcha permite a los administradores implementar varios tipos de control de acceso, tal como se ilustra en los siguientes ejemplos.

Tabla 1. Ejemplos de control de acceso con reescritura de consultas.

Control de acceso	SQL original	SQL reescrito
Limitación del acceso a filas mediante la adición de una cláusula WHERE	`SELECT C from T`	`SELECT C from T WHERE [valores]`
Limitación del acceso a columnas modificando la lista SELECT	`SELECT C1 from T`	`SELECT C2 from T`
	`SELECT C1,C2 from T`	`SELECT C2 from T`
Restricción de actividades de base de datos mediante la reescritura de sentencias de SQL para no hacer nada	`SELECT EMAIL from T`	`SELECT++ EMAIL from T`
Restricción de lo que pueden hacer los usuarios mediante la modificación de verbos de consulta (SELECT, INSERT, UPDATE, etc.)	`DROP TABLE T`	`UPDATE T SET [valores]`
Restricción de lo que pueden hacer los usuarios mediante la modificación de objetos de consulta (TABLE, VIEW, COLUMN, etc.)	`SELECT C from T1`	`SELECT C from T2`

La posibilidad de reescribir de forma automática las consultas de base de datos proporciona un mecanismo extremadamente potente y flexible de control de acceso que permite a las organizaciones abordar rápidamente una amplia gama de problemas de seguridad. Por ejemplo, las definiciones de reescritura de consultas se pueden desarrollar para lograr cualquiera de los siguientes objetivos:

- Imponer la seguridad en escenarios de multitularidad donde varios usuarios y aplicaciones comparten una única base de datos, pero donde no todos los usuarios y aplicaciones deberían tener acceso a todos los datos
- Exponer una base de datos a un entorno de producción con fines de prueba sin exponer toda la base de datos.
- Corregir rápidamente las vulnerabilidades de seguridad críticas mientras se desarrollan soluciones permanentes a nivel de aplicación o de base de datos.

Revise las secciones siguientes para obtener más información sobre cómo funciona la reescritura de consultas y cómo configurarla para su uso dentro del entorno de Guardium.

Nota: Si se ha configurado al S-TAP con firewall_default_state=1, no es posible establecer al mismo tiempo el estado predeterminado para la reescritura de consultas, qrw_default_state=1.

- Cómo funciona la reescritura de consultas
  Conozca cómo Guardium implementa la funcionalidad de reescritura de consultas.
- Utilización de la reescritura de consultas
  Aprenda a habilitar y utilizar la funcionalidad de reescritura de consultas.

Tema principal: Protección

Cómo funciona la reescritura de consultas

Conozca cómo Guardium implementa la funcionalidad de reescritura de consultas.

Visión general

Una vez que se ha habilitado la reescritura de consultas en el S-TAP para los servidores de bases de datos soportados (consulte Habilitación de la reescritura de consultas), la funcionalidad de reescritura de consultas se implementa a través de tres acciones de reglas de política:

- REESCRITURA DE CONSULTA: ADJUNTAR
- REESCRITURA DE CONSULTA: APLICAR DEFINICIÓN

- REESCRITURA DE CONSULTA: DESADJUNTAR

Estas acciones de regla se instalan como reglas de política de acceso. Las reglas de política de acceso especifican tanto las definiciones de reescritura de consultas que indican cómo se deben reescribir las consultas como un contexto de tiempo de ejecución que indica cuándo se deben aplicar dichas definiciones.

Una vez que se han especificado las reglas de reescritura de consultas, las sesiones se manejan del modo siguiente:

1. Una solicitud SQL desencadena una regla REESCRITURA DE CONSULTA: ADJUNTAR, y toda la actividad posterior en la sesión se observa para la reescritura de consultas.
2. Mientras las sesiones se observan para la reescritura, el tráfico se aloja en el S-TAP y la información de la sesión se comprueba con relación a reglas de políticas de acceso.
3. Si una consulta en la sesión observada coincide con una regla REESCRITURA DE CONSULTA: APLICAR DEFINICIÓN, la consulta se reescribe de acuerdo con la definición y se envía al S-TAP.
4. El S-TAP libera la consulta reescrita al servidor de bases de datos.
5. Cuando se desencadena una regla REESCRITURA DE CONSULTA: DESADJUNTAR, la reescritura de consulta deja de observar la actividad durante el resto de la sesión o hasta que se desencadena otra regla REESCRITURA DE CONSULTA: ADJUNTAR.

Requisitos y limitaciones

La reescritura de consultas está pensada para trabajar con los servidores de bases de datos siguientes:

- Oracle
- DB2 (solo Linux y Unix)
- Microsoft SQL

Para obtener información sobre los servidores de bases de datos soportados y las restricciones asociadas, consulte Plataformas soportadas para IBM Guardium 10.1. Para obtener información detallada sobre el soporte de cliente de base de datos para la reescritura de consultas, póngase en contacto con el soporte de IBM Guardium.

Importante: Cuando la reescritura de consultas observa una sesión, el sniffer debe enviar veredictos del motor a S-TAP para cada solicitud de SQL en la sesión. Este proceso es asíncrono e incorpora una latencia entre el sniffer y el S-TAP. Cree condiciones de regla de reescritura de consulta que eviten adjuntarse a sesiones para aplicaciones de confianza o sensibles al rendimiento.
Tema principal: Reescritura de consultas
Tareas relacionadas:
Habilitación de la reescritura de consultas

Utilización de la reescritura de consultas

Aprenda a habilitar y utilizar la funcionalidad de reescritura de consultas.

Acerca de esta tarea

Siga esta secuencia de tareas para habilitar y empezar a utilizar la funcionalidad de reescritura de consultas.

1. Habilitación de la reescritura de consultas
   Aprenda a configurar un S-TAP para la funcionalidad de reescritura de consultas.
2. Creación de definiciones de reescritura de consultas
   Aprenda a crear definiciones de reescritura de consultas para escenarios de enmascaramiento de datos y control de acceso.
3. Cómo probar las definiciones de reescritura de consulta
   Obtenga información sobre cómo probar las definiciones de reescritura de consulta con relación a la entrada de ejemplo y verificar que las definiciones de reescritura se comportan según lo esperado.
4. Definición de una política de seguridad para activar la reescritura de consultas
   Aprenda a crear reglas de política de acceso utilizando las definiciones de reescritura de consulta con consultas activas.
5. Creación de un informe personalizado para validar los resultados de la reescritura de consultas
   Aprenda a crear un informe de seguimiento de reescritura de consultas para auditar la actividad de la reescritura de consultas.

Tema principal: Reescritura de consultas

Habilitación de la reescritura de consultas

Aprenda a configurar un S-TAP para la funcionalidad de reescritura de consultas.

Acerca de esta tarea

La funcionalidad de reescritura de consulta únicamente se habilitada cuando se cumplen las dos condiciones siguientes:

- La reescritura de consultas está habilitada en el archivo guard_tap.ini
- Existen reglas de política de reescritura de consulta que son desencadenadas por el tráfico de la sesión

Esta tarea le guía a través de los cambios que necesita realizar en el archivo guard_tap.ini.

Procedimiento

1. Abra guard_tap.ini en un editor de texto.
2. Localice el parámetro qrw_installed = 0 y cámbielo a qrw_installed = 1. El parámetro qrw_installed debe establecerse en un valor de 1 para habilitar la funcionalidad de reescritura de consultas. Establezca qrw_installed = 0 para inhabilitar la funcionalidad de reescritura de consultas.
3. Guarde los cambios en guard_tap.ini.
4. En el sistema Guardium, inicie la sesión como usuario de CLI y reinicie el motor de inspección utilizando el mandato de CLI restart_inspection_engines.

Resultados

Cuando haya completado esta tarea, la funcionalidad de reescritura de consultas estará habilitada y responderá a reglas de política que contengan acciones de reescritura de consulta.
Tema principal: Utilización de la reescritura de consultas
Tema siguiente: Creación de definiciones de reescritura de consultas

Creación de definiciones de reescritura de consultas

Aprenda a crear definiciones de reescritura de consultas para escenarios de enmascaramiento de datos y control de acceso.

Procedimiento

1. Abra Proteger > Políticas de seguridad > Creador de reescritura de consultas.
2. Proporcione un nombre exclusivo con sentido para la definición de reescritura de consulta en el campo Nombre.
3. Cree y analice una consulta de modelo.
   a. Proporcione una consulta de modelo en el campo Especificar una consulta de modelo.

      Por ejemplo, para crear una definición de reescritura que impida el uso de las sentencias `SELECT * from`, especifique `SELECT * from EMPLOYEE` como modelo.

   b. Pulse el menú Tipo de BD y seleccione un analizador de SQL para utilizarlo con la consulta de modelo.
   c. Pulse Analizar para procesar la consulta de modelo.

      La consulta de modelo se descompondrá en componentes individuales con cada componente accionable resaltado con texto subrayado.

4. Defina cómo se deben reescribir los componentes específicos de la consulta de modelo.
   a. Pulse en un componente subrayado de la consulta analizada que le gustaría reescribir. Se abrirá un diálogo que le ayudará a crear su definición de reescritura de consulta.

      Opciones:

      - Seleccione y modifique un verbo, campo u objeto individual a partir de la consulta analizada
      - Añada un componente a la consulta (se muestra como texto subrayado gris junto a la consulta analizada)
      - Reescriba toda la consulta pulsando la [R] subrayada de color gris junto a la consulta analizada.

      En el ejemplo `SELECT * from EMPLOYEE`, donde queremos impedir el uso de sentencias `SELECT * from`, pulse el * para proporcionar un contenido reescrito.

   a. El campo Cambio desde indica lo que será reescrito.
   b. El campo A define el componente reescrito.

      Por ejemplo, para impedir el uso de sentencias `SELECT * from`, sustituya el componente `*` con una lista de objetos específicos: `EMPNO, FIRSTNME, MIDINIT, LASTNAME, WORKDEPT, PHONENO, HIREDATE, JOB, EDLEVEL, SEX`.

      Importante:

      Las definiciones de reescritura se basan en la sintaxis, por lo que cualquier sentencia con el formato `SELECT * from [OBJETO]` coincidirá con el ejemplo. Por ejemplo, las sentencias `SELECT * from DEPARTMENT` y `SELECT * from EMPLOYEE` se aplican a este ejemplo.

      Las definiciones de reescritura de consulta se pueden restringir a objetos específicos utilizando reglas de política de acceso. Consulte Definición de una política de seguridad para activar la reescritura de consultas para obtener más información.

   c. Pulse Guardar para guardar la definición de reescritura y, a continuación, pulse Atrás para cerrar el diálogo.
5. Revise la salida de la definición de la reescritura de consulta utilizando el campo Vista previa en tiempo real y realice los cambios que sean necesarios.

   Siguiendo este ejemplo, `SELECT * from EMPLOYEE` se reescribirá como `SELECT EMPNO, FIRSTNME, MIDINIT, LASTNAME, WORKDEPT, PHONENO, HIREDATE, JOB, EDLEVEL, SEX from EMPLOYEE`.

6. Cuando esté satisfecho con los resultados, pulse Guardar para guardar la definición de la reescritura de consulta.

   La definición de reescritura de consulta se guarda y se visualiza en la lista de definiciones de reescritura de consulta disponibles en el Creador de reescritura de consulta.

Qué hacer a continuación

Continúe trabajando con las definiciones de reescritura de consulta:

- Cree definiciones adicionales pulsando Nueva y repita los pasos de esta tarea.
- Edite una definición de reescritura de consulta existente efectuando una doble pulsación en un elemento de la lista de definiciones de reescritura de consulta disponibles.
- Copie y edite una definición de reescritura de consulta existente seleccionando el elemento en la lista de definiciones de reescritura de consulta disponibles y pulse Clonar.
- Suprima una definición de reescritura de consulta existente seleccionando el elemento en la lista de definiciones de reescritura de consulta disponibles y pulse Suprimir.

Cuando haya terminado de trabajar con definiciones de reescritura de consulta, continúe con el paso siguiente de esta secuencia para probar e implementar las definiciones.
Tema principal: Utilización de la reescritura de consultas
Tema anterior: Habilitación de la reescritura de consultas
Tema siguiente: Cómo probar las definiciones de reescritura de consulta
Tareas relacionadas:
Definición de una política de seguridad para activar la reescritura de consultas

Cómo probar las definiciones de reescritura de consulta

Obtenga información sobre cómo probar las definiciones de reescritura de consulta con relación a la entrada de ejemplo y verificar que las definiciones de reescritura se comportan según lo esperado.

Antes de empezar

Para completar esta tarea, necesita haber creado una o varias definiciones de reescritura de consulta.

Procedimiento

1. Abra Proteger > Políticas de seguridad > Creador de reescritura de consultas.
2. Pulse Configuración de prueba para abrir un diálogo y seleccionar las definiciones de reescritura de consulta para realizar las pruebas.
   a. Arrastre y suelte los elementos desde el campo Definiciones de reescritura de consulta disponibles en el campo Probar definiciones de reescritura de consulta.
   b. Arrastre y suelte elementos con en el campo Probar definiciones de reescritura de consulta para ordenar varias definiciones tal como lo haría dentro de una política de acceso.
   c. Pulse Guardar para cerrar el diálogo cuando haya terminado.
3. Escriba o pegue las consultas de prueba en el campo de prueba.

   Por ejemplo, para probar una definición de reescritura que impide el uso de sentencias `SELECT * from`(consulte la sección Creación de definiciones de reescritura de consultas), especifique consultas de ejemplo, como:

```
SELECT * from DEPARTMENT
SELECT * from EMPLOYEE
SELECT FIRSTNME, case
when SALARY > 150000 then 'high'
when SALARY > 100000 then 'medium'
when SALARY > 80000 then 'fair'
else 'poor'
end from EMPLOYEE
DELETE from EMPLOYEE where EMPNO=100
INSERT into TEMP_EMP SELECT * from EMPLOYEE
```

4. Pulse Ejecutar prueba para procesar las consultas de ejemplo y revisar los resultados.

   Por ejemplo, las consultas de ejemplo proporcionadas en el paso anterior devuelven los resultados siguientes:

Tabla 1. Resultados de la prueba de reescritura de consulta

SQL original	SQL reescrito	Cambiado
`SELECT * from DEPARTMENT`	`SELECT EMPNO, FIRSTNME, MIDINIT, LASTNAME, WORKDEPT, PHONENO, HIREDATE, JOB, EDLEVEL, SEX from DEPARTMENT`	SÍ
`SELECT * from EMPLOYEE`	`SELECT EMPNO, FIRSTNME, MIDINIT, LASTNAME, WORKDEPT, PHONENO, HIREDATE, JOB, EDLEVEL, SEX from EMPLOYEE`	SÍ
`SELECT FIRSTNME, case when SALARY > 150000 then 'high' when SALARY > 100000 then 'medium' when SALARY > 80000 then 'fair' else 'poor' end from EMPLOYEE`	`SELECT FIRSTNME, case when SALARY > 150000 then 'high' when SALARY > 100000 then 'medium' when SALARY > 80000 then 'fair' else 'poor' end from EMPLOYEE`	NO
`DELETE from EMPLOYEE where EMPNO=100`	`DELETE from EMPLOYEE where EMPNO=100`	NO
`INSERT into TEMP_EMP SELECT * from EMPLOYEE`	`INSERT into TEMP_EMP SELECT * from EMPLOYEE`	NO

Importante:

Las definiciones de reescritura se basan en la sintaxis, por lo que cualquier sentencia con el formato `SELECT * from [OBJETO]` coincidirá con el ejemplo. Por ejemplo, las sentencias `SELECT * from DEPARTMENT` y `SELECT * from EMPLOYEE` se aplican a este ejemplo.

Las definiciones de reescritura de consulta se pueden restringir a objetos específicos utilizando reglas de política de acceso. Consulte Definición de una política de seguridad para activar la reescritura de consultas para obtener más información.

5. Continúe especificando consultas de ejemplo para probar las definiciones de reescritura. Pulse Configuración de prueba para cambiar o reordenar las definiciones de reescritura utilizadas para la prueba.

Qué hacer a continuación

Cuando esté satisfecho con los resultados de la prueba, cree una política de seguridad para empezar a utilizar sus definiciones de reescritura de consulta con consultas activas.

Tema principal: Utilización de la reescritura de consultas
Tema anterior: Creación de definiciones de reescritura de consultas
Tema siguiente: Definición de una política de seguridad para activar la reescritura de consultas
Tareas relacionadas:
Definición de una política de seguridad para activar la reescritura de consultas
Creación de definiciones de reescritura de consultas

Definición de una política de seguridad para activar la reescritura de consultas

Aprenda a crear reglas de política de acceso utilizando las definiciones de reescritura de consulta con consultas activas.

Antes de empezar

Para completar esta tarea, debe haber creado y probado una o varias definiciones de reescritura de consulta y debe estar familiarizado con la creación de políticas de seguridad.

Procedimiento

1. Abra Proteger > Políticas de seguridad > Creador de políticas
2. Cree una nueva política o modifique una política existente para utilizar con sus definiciones de reescritura de consulta.
   Consejo: Considere la posibilidad de crear una nueva política para probar las definiciones de reescritura de consulta. Añada las reglas de reescritura a las políticas de seguridad existentes una vez que esté satisfecho con el comportamiento de la política de prueba.
3. Pulse Editar reglas para empezar a añadir reglas de reescritura a la política seleccionada y, a continuación, seleccione Añadir reglas > Añadir regla de acceso.
   Nota: Las reglas de reescritura de consulta se clasifican siempre como reglas de acceso.
4. Añada una regla con una acción de regla REESCRITURA DE CONSULTA: ADJUNTAR. Asegúrese de marcar el recuadro de selección Continuar en la siguiente regla. Esta regla identifica los parámetros de sesión específicos que deben coincidir para desencadenar una sesión de reescritura de consulta, por ejemplo, un nombre de usuario de base de datos o una dirección IP de cliente específica.
5. Añada una regla con una o más acciones de regla REESCRITURA DE CONSULTA: APLICAR DEFINICIÓN y seleccione la definición o definiciones de reescritura de consulta que desee aplicar. Asegúrese de marcar el recuadro de selección Continuar en la siguiente regla. Esta regla identifica los mandatos u objetos específicos que deben coincidir para aplicar las definiciones de reescritura y modificar la consulta de origen.

   Por ejemplo, si se establece el campo Objeto en `EMPLOYEE`, se restringe una definición de reescritura `SELECT * from` a objetos `EMPLOYEE`.

6. Añada una regla con una acción de regla REESCRITURA DE CONSULTA: DESADJUNTAR. Esto cierra la sesión de reescritura de consultas e impide la supervisión adicional del tráfico de la sesión.
7. Para instalar la nueva política, vuelva al Buscador de políticas, seleccione su política de seguridad y elija Seleccionar una acción de instalación > Instalar y modificar. Pulse Aceptar cuando se le solicite que confirme la instalación de la política.
8. Inicie la sesión en el servidor de bases de datos y ejecute las consultas de prueba para verificar que las reglas de reescritura de política están funcionando tal como estaba previsto.
   a. Inicie una sesión en el servidor de la base de datos.
   b. Emita consultas que deban desencadenar (o no deban desencadenar) las reglas de política de acceso instaladas y que coincidan con los criterios de las definiciones de reescritura de consulta.

      Por ejemplo, emita `SELECT * from EMPLOYEE` para verificar que una definición de reescritura de `SELECT * from` se aplica al objeto `EMPLOYEE`, y emita `SELECT * from DEPARTMENT` para verificar que la misma definición no se aplica al objeto `DEPARTMENT`.

   c. Verifique que los resultados reflejan el SQL reescrito.

Tema principal: Utilización de la reescritura de consultas
Tema anterior: Cómo probar las definiciones de reescritura de consulta
Tema siguiente: Creación de un informe personalizado para validar los resultados de la reescritura de consultas
Conceptos relacionados:
Políticas

Creación de un informe personalizado para validar los resultados de la reescritura de consultas

Aprenda a crear un informe de seguimiento de reescritura de consultas para auditar la actividad de la reescritura de consultas.

Antes de empezar

Para completar esta tarea, debe haber creado e instalado reglas de política de acceso que apliquen definiciones de reescritura de consulta. También debe estar familiarizado con la creación de informes.

Acerca de esta tarea

Un informe de seguimiento de reescritura de consultas ayuda a validar las acciones de reescritura, tanto en los entornos de producción como en los de prueba.

Procedimiento

1. Abra Informes > Herramientas de configuración de informes > Creador de consultas
2. Seleccione Reescritura de consultas desde el menú Dominio.
3. Pulse el icono para definir una nueva consulta.
4. Proporcione un nombre exclusivo con sentido para la consulta en el campo Nombre de consulta.

   Por ejemplo, `Mi informe de reescritura de consulta`

5. Seleccione una de las opciones disponibles en el menú Entidad principal.

   Están disponibles las opciones siguientes:

   - Registro de reescritura de consulta
   - Cliente/Servidor
   - Sesión
   - Periodo de acceso

6. Pulse Siguiente para abrir el creador de informes.
7. Expanda secciones dentro de la Lista de entidades y seleccione elementos para crear su informe.
   - Pulse un elemento y seleccione Añadir campo para añadir el elemento como una columna en el informe.
   - Pulse un elemento y seleccione Añadir condición para añadir un filtro condicional al informe.
   - Como alternativa, arrastre y suelte elementos de la Lista de entidades en las tablas Campos de consulta y Condiciones de consulta para aplicarlas al informe.

   Incluya los elementos siguientes como un punto de partida para un informe de reescritura de consultas:

- Cliente/Servidor: Indicación de fecha y hora
- Cliente/Servidor: Nombre de usuario de BD
- Cliente/Servidor: Tipo de servidor
- Registro de reescritura de consultas: Nombres de definición de reescritura de consultas aplicados
- Registro de reescritura de consultas: SQL de entrada
- Registro de reescritura de consultas: SQL de salida

8. Pulse Guardar cuando haya terminado de crear el informe.
9. Pulse Crear informe para crear el informe.
10. Pulse Añadir a mis informes personalizados para añadir el informe a sus informes personalizados.
11. Abra Informes > Mis informes personalizados y seleccione el informe que ha creado para ver un informe de las acciones de reescritura de consultas.

Tema principal: Utilización de la reescritura de consultas
Tema anterior: Definición de una política de seguridad para activar la reescritura de consultas

Reglas y políticas de la actividad de archivos

La supervisión de la actividad de archivos garantiza la integridad y la protección de los datos confidenciales en servidores de archivos UNIX y Windows.

- Funcionalidad de reglas y políticas de actividad de archivos
  Una política de supervisión de actividad de archivo especifica indica a Guardium la forma en la que manejar los distintos sucesos de actividad de archivo. Cada política consta de un conjunto ordenado de reglas. Cada regla en una política define una acción condicional que se toma cuando se cumple la regla. La prueba condicional puede ser simple, por ejemplo un acceso de usuario a una ubicación específica, o una prueba compleja que considere varias condiciones. La acción abarca desde no hacer nada a bloquear el suceso. Se pueden combinar y ordenar varias acciones de agrupación y alerta para crear respuestas sofisticadas a reglas coincidentes.
- Creación de una nueva política de FAM y de sus reglas
  Configure la supervisión de actividad de archivos definiendo y gestionando reglas y políticas en la ventana Creador de políticas para archivos.
- Creación de una regla de política de FAM desde el separador de titularidades del Panel de control de investigación
  Puede utilizar los datos supervisados como, por ejemplo, nombres de origen de datos, nombres de usuario, acciones y vías de acceso de archivo, en la Tabla de resultados del Panel de control de investigación para crear reglas de política.

Tema principal: Protección
Información relacionada:
Supervisión de la actividad de archivos utilizando Guardium (vídeo).

Funcionalidad de reglas y políticas de actividad de archivos

Una política de supervisión de actividad de archivo especifica indica a Guardium la forma en la que manejar los distintos sucesos de actividad de archivo. Cada política consta de un conjunto ordenado de reglas. Cada regla en una política define una acción condicional que se toma cuando se cumple la regla. La prueba condicional puede ser simple, por ejemplo un acceso de usuario a una ubicación específica, o una prueba compleja que considere varias condiciones. La acción abarca desde no hacer nada a bloquear el suceso. Se pueden combinar y ordenar varias acciones de agrupación y alerta para crear respuestas sofisticadas a reglas coincidentes.

Por ejemplo, puede definir políticas para estos casos:

- Registrar una infracción de política si John escribe en la carpeta CONFIDENTIAL
- Bloquear a un grupo de usuarios para que no puedan suprimir el archivo SALARIES.XLS
- Enviar un correo electrónico a Krishna si JENNY lee cualquier archivo que empiece por sample*
- Auditar todos los accesos a archivos clasificados con datos confidenciales relacionados con PCI

Grupos: Guardium utiliza el concepto de grupos para la creación de informes y políticas.

Los grupos Guardium se crean y mantienen en el recopilador de Guardium o en el Gestor central (CM). No confunda los grupos de Guardium con los grupos de sistemas de archivos.

Es recomendable que considere una estrategia de denominación para los grupos, incluidos grupos de orígenes de datos (servidores de archivos), grupos de archivos (por ejemplo por nivel de confidencialidad o por una combinación de nivel de confidencialidad y aplicación) o grupos de usuarios (una lista de todos los usuarios conocidos, usuarios "autorizados" y usuarios con privilegios especiales).

Directrices para las reglas

- Una regla demasiado amplia (una regla que supervisa demasiados archivos) puede sobrecargar el sistema e incrementar el tiempo de respuesta y proceso.
- Una regla de FAM puede incluir más de un patrón. Para proteger tanto un directorio como su contenido, defina una regla con dos patrones: /FAMtest/* y /FAMtest.
- Grupos formados con vías de acceso de archivo: cada vía de acceso debe ser única sin tener en cuenta las mayúsculas y minúsculas. Por ejemplo, estas dos vías de acceso pueden coexistir en un grupo: C:\ABC y C: \abcdef. Sin embargo, estas dos vías de acceso no pueden coexistir en un grupo C:\ABC y C: \abc. El Creador de grupos no es sensible a las mayúsculas y minúsculas. No es necesario especificar miembros con todos los caracteres en mayúsculas o todos en minúsculas. Sin embargo, en UNIX, que es sensible a las mayúsculas y minúsculas, la vía de acceso /IBM/Guardium es distinta de la vía de acceso /ibm/guardium. Si el usuario desea supervisar ambas vías de acceso, el Creador de grupos actual tiene una limitación y no las verá como dos vías de acceso.
- El orden de las reglas en la política de seguridad es muy importante. Las reglas se envían al S-TAP como un conjunto y se procesan exactamente según el orden establecido. Toda la actividad de los usuarios se comprueba con relación a cada regla en la política según el orden de dichas reglas. La primera regla que cumpla los criterios de este acceso de archivo se aplica y las reglas siguientes se ignoran. En la mayoría de los casos, coloque en primer lugar la regla más específica al principio y la regla más general al final. Por ejemplo, si tienes dos reglas:
  - **Regla A:** *sólo auditar* todo el acceso a /data/*
  - **Regla B:** *bloquear, registrar infracción y auditar* al usuario 'joe' de acceder a /data/salaries

  Si primero coloca la regla A y Joe intenta leer /data/salaries, no habrá necesidad de ir a la regla siguiente, y Joe será auditado. Si coloca en primer lugar la Regla B, a Joe se le bloquea el acceso a /data/salaries y no habrá necesidad de ir a la siguiente regla.

Comportamiento de FAM utilizando un S-TAP anterior a la versión 10.1.2 (sin soporte de múltiples acciones) con un sniffer de la versión 10.1.2 o superior (incluye soporte a múltiples acciones)

- Si está utilizando un S-TAP anterior a la versión 10.1.2 con una nueva interfaz de usuario/sniffer de la versión 10.1.2 con reglas de múltiples acciones, el bloqueo se implementa de forma correcta puesto que está acción se lleva a cabo en el lado del S-TAP.

- En el lado del Sniffer, las acciones son acumulativas para todas las acciones especificadas.
- Por ejemplo, si selecciona Sólo auditoría para el mandato READ y Bloquear, Registrar infracciones y Auditar para el mandato DELETE, entonces se bloquea el mandato DELETE, pero no el mandato READ. Sin embargo, tanto el mandato READ como el mandato DELETE desencadenan auditar, registrar infracciones y alertas a pesar de que el mandato READ era de Solo auditaría.
- En el otro caso en el que el usuario utiliza un S-TAP de la versión 10.1.2 y una interfaz de usuario/Sniffer de una versión anterior a la versión 10.1.2, el funcionamiento será el adecuado puesto que no hay forma de definir una regla de múltiples acciones (por tanto no hay interfaz de usuario ni GuardAPI para soportar).

Atributos de regla

Nombre de regla

Un nombre exclusivo

Origen de datos

El origen de datos puede ser:

- Un origen de datos seleccionado de la lista desplegable
- Un grupo seleccionado de la lista desplegable
- Un grupo creado a partir de grupos seleccionados en la ventana Crear nueva regla
- Una vía de acceso especificada manualmente

Acción de regla

La acción de regla es la acción que se lleva a cabo cuando se cumplen los criterios. Las acciones son una de las siguientes:

- Una acción para cualquier acceso a archivo que coincida con los criterios de la regla
- Una regla de múltiples acciones comprende varias acciones, cada una para una categoría de mandato especifica o un grupo específico. Tenga en cuenta que la opción **Continuar en la siguiente regla** no está soportada cuando se utilizan reglas de múltiples acciones.

Las acciones de regla son:

- Alerta y auditoría: enviar una alerta directamente generada desde el sniffer con un comportamiento específico, y registrar el suceso.
- Solo auditoría: Registrar el suceso en las tablas de GDM
- Bloquear, registrar infracción y auditar: Bloquear el acceso al objeto, registrar una infracción de política y registrar el suceso. Una acción de bloqueo también requiere una configuración de alerta.
- Ignorar: No toma ninguna acción.
- Registrar como infracción y auditar: Registrar esta infracción de política y registrar el suceso.

Mandatos de acceso: Puesto que hay cientos de mandatos del sistema de archivos, se agrupan en estas categorías:

- Lectura
- Escritura
- Ejecución
- Supresión
- Operación de archivo, incluye todas las llamadas que afectan a los metadatos de archivo como, por ejemplo, cambiar la propiedad del archivo, cambiar los permisos del archivo y llamadas similares.

Estas categorías están prefijadas en el sistema y no se pueden cambiar. Sin embargo, puede crear un grupo Guardium que contenga cualquier combinación de categorías, y utilizar ese grupo en la política de seguridad. Por ejemplo, puede crear un grupo Guardium que contenga a Ejecutar y Escribir como miembros.

Si deja el mandato sin especificar, se contarán como coincidencia todos los mandatos del sistema de archivos. Algunas llamadas como, por ejemplo, para obtener la hora del sistema, no afectan a los archivos y se ignoran.

Criterio de regla

Para cualquier acceso de archivo dado, se utilizan criterios de regla para evaluar si se debe realizar una acción determinada. Para cualquier origen de datos o grupo de orígenes de datos (servidores de archivos), los criterios de regla que puede especificar incluyen:

Usuario: Usuario de SO que está accediendo a los archivos. También puede ser un grupo de usuarios, tal como se define en un grupo Guardium. Si se deja en blanco, la regla se aplica a todos los usuarios (excepto a root).

Vía de acceso de archivo: Puede ser una vía de acceso de archivo de Windows o UNIX, una vía de acceso de archivo individual o un grupo de vías de acceso de archivo, tal como se ha definido en un grupo Guardium. No puede estar en blanco (excepto cuando se selecciona un soporte de almacenamiento extraíble). También puede seleccionar supervisar los subdirectorios en la vía de acceso de los archivos.

Comodines en la especificación de los nombres:

- El carácter '*' coincide con un número cualquiera de caracteres
- El carácter '?' coincide con un único carácter
- Con UNIX, utilice la barra inclinada invertida para crear secuencias de escape para * y ?

Consejo: Los caracteres de comodín precisan de un proceso adicional. El uso excesivo de comodines afecta al rendimiento.

UNIX

Uso:

Para una coincidencia con todos los archivos en el disco, especifique /*

Para una coincidencia exacta de /tmp/My*File.txt, utilice /tmp/My*File.txt

Para una coincidencia con los archivos con la extensión .txt en /tmp, utilice /tmp/*.txt

Ejemplo: El patrón de regla de FAM es: /FAM*

significado

- Directorio: /
- Nombre de archivo: FAM*

La regla en curso tiene seleccionados subdirectorios: (Subdirectorios: Sí)

El archivo al que se accede es:

/guardium/modules/SUPERVISOR/10.0.0/FAM.output

Hay una coincidencia. El nombre de archivo, FAM.output, coincide con el nombre, FAM, y está ubicado en el subdirectorio del directorio dado '/'.

Windows: Para Windows, debe especificar la unidad, como por ejemplo C:\

Uso:

Para supervisar todos los archivos de la unidad C, especifique C:\ y marque el recuadro de selección Supervisar subdirectorios.

Para una coincidencia con los archivos con la extensión .txt en C:\tmp, utilice C:\tmp*.txt

Ejemplos de GuardAPI: crear una política con dos reglas

```
grdapi create_policy ruleSetDesc=policy1 isFam=true
grdapi create_fam_rule policyName=policy1 ruleName=rule1 serverHost="x.x.x.x" filePath="/famtest/*" command="DELETE"
actionName="Alert and Audit" notificationType="SYSLOG"
grdapi create_fam_rule policyName=policy1 ruleName=rule2 serverHost="x.x.x.x" filePath="/famtest/*" command="READ"
actionName="Alert and Audit" notificationType="MAIL"
```

policy1 -> rule1 -> "DELETE" -> "Alert and Audit" -> "SYSLOG"

policy1 -> rule2 -> "READ" -> "Alert and Audit" -> "MAIL"

Ejemplos de GuardAPI: crear una política con una regla de múltiples acciones

Regla de múltiples acciones para FAM: Las reglas de múltiples acciones comprenden varias acciones, cada una para una categoría de mandato especifica o un grupo específico. Los mandatos en un contexto de FAM son: Leer, Escribir, Suprimir, Ejecutar y Operación de archivo. Si el sistema no da soporte a reglas de múltiples acciones, pasa por alto la regla y continúa con la regla siguiente.

```
grdapi create_policy ruleSetDesc=policy1 isFam=true
grdapi create_fam_rule policyName=policy1 ruleName=rule1 serverHost="x.x.x.x" filePath="/famtest/*"
add_action_to_fam_rule policyName=policy1 ruleName=rule1 command="DELETE, READ" actionName="Alert and Audit"
notificationType="SYSLOG"
add_action_to_fam_rule policyName=policy1 ruleName=rule1 command="WRITE" actionName="Alert and Audit" notificationType="MAIL"
```

policy1 -> rule1 -> "DELETE, READ" -> "Alert and Audit" -> "SYSLOG"

policy1 -> rule1 -> "WRITE" -> "Alert and Audit" -> "MAIL"

Adding another action using commandGroupId, assuming commandGroupId=20000 exists, and it has "DELETE, WRITE"

```
add_action_to_fam_rule policyName=policy1 ruleName=rule1 command="READ" commandGroupId=20000 actionName="Ignore"
notificationType=""
```

policy1 -> rule1 -> "READ, DELETE, WRITE" -> "Ignore"

Comportamiento de FAM con S-TAP anteriores a la versión 10.1.2 y sniffers de la versión 10.1.2 y superior

Las reglas de múltiples acciones para FAM se introdujeron en S-TAP de la versión 10.1.2. S-TAP anteriores a la versión 10.1.2 no dan soporte a múltiples acciones de FAM, que los sniffers de la versión 10.1.2 y superior si lo hacen. En el lado del Sniffer, las acciones son acumulativas para todas las acciones especificadas.

Por ejemplo, si la política especifica Sólo auditoría para el mandato READ y Bloquear, Registrar infracciones y Auditar para el mandato DELETE, entonces se bloquea el mandato DELETE, pero no el mandato READ. Sin embargo, tanto el mandato READ como el mandato DELETE desencadenarán auditar, registrar infracciones y alertas a pesar de que el mandato READ era de Solo auditar.

Tema principal: Reglas y políticas de la actividad de archivos

Creación de una nueva política de FAM y de sus reglas

Configure la supervisión de actividad de archivos definiendo y gestionando reglas y políticas en la ventana Creador de políticas para archivos.

Acerca de esta tarea

Una vez abra el Creador de políticas para archivos, y vistas adicionales dentro del creador de políticas, podrá conmutar entre las distintas vistas pulsando Creador de políticas para archivos, Nueva política y Crear nueva regla en la parte inferior de la página.

También puede crear políticas y reglas con GuardAPI.

Procedimiento

1. En una unidad gestionada (MU) o autónoma, para acceder al creador de políticas de FAM, vaya a Proteger > Políticas de seguridad > Creador de políticas para archivos.
2. Especifique un nombre para la nueva política. (Podrá guardar la política una vez se haya definido una regla).
3. Para añadir reglas existentes a la política.
   a. Pulse Mostrar plantillas. Se abre la tabla Plantillas de reglas.
   b. Opcionalmente, filtre la lista con la función de filtro.
   c. Seleccione una o más reglas y pulse la flecha derecha

4. Para crear una nueva regla.
    a. Pulse para abrir la ventana Crear nueva regla.
    b. Asigne un nombre a la regla, defina sus atributos y pulse en Guardar.
5. Para modificar una regla existente y añadirla a la política.
    a. Seleccione la regla y pulse .
    b. Pulse , cambie el nombre, modifique otros atributos según sea necesario y pulse Guardar.
6. Cambie el orden de las reglas utilizando
7. Suprima una regla seleccionándola y pulsando suprimir regla.
8. Pulse Guardar para guardar la política, o Guardar e instalar para instalar la política de forma inmediata. (Consulte Instalación de políticas).

Tema principal: Reglas y políticas de la actividad de archivos
Información relacionada:
Funciones de GuardAPI File Activity Monitor

Creación de una regla de política de FAM desde el separador de titularidades del Panel de control de investigación

Puede utilizar los datos supervisados como, por ejemplo, nombres de origen de datos, nombres de usuario, acciones y vías de acceso de archivo, en la Tabla de resultados del Panel de control de investigación para crear reglas de política.

Antes de empezar

- El paquete FAM debe estar instalado y configurado
- El descubrimiento y la clasificación deben estar habilitados
- El Panel de control de investigación debe estar habilitado, consulte Habilitación e inhabilitación del panel de control de investigación

Acerca de esta tarea

Procedimiento

1. Elija Archivo en la lista desplegable en el mensaje de cabecera del producto y pulse el icono de búsqueda para abrir el Panel de control de investigación para los datos de archivo.
2. Abra el separador de Titularidades de la Tabla de resultados. Pulse en Detalles para ver entradas individuales.
3. Elija una o varias entradas en los resultados que desee utilizar para cumplimentar una regla. Utilice el recuadro de selección Seleccionar todo para incluir todas las entradas que se visualizan actualmente (no todas las entradas de la base de datos).
4. Pulse con el botón de la derecha y elija Añadir regla de política. Se abre el diálogo Crear regla con los valores de las entradas que ha seleccionado. Si ha seleccionado varias entradas, se crea un grupo que contiene los valores de dichas entradas. Puede crear una regla para añadirla a una política existente, o puede crear una nueva política que incluya su nueva regla.
   Nota: Una regla demasiado amplia (una regla que supervisa demasiados archivos) sobrecargará el sistema e incrementará el tiempo de respuesta y proceso.
   Nota: Una regla de FAM puede incluir más de un patrón. Para proteger tanto un directorio como su contenido, defina una regla con dos patrones: /FAMtest/* y /FAMtest.
   Nota: Cuando se utiliza una política de FAM, el establecer un grupo para definir vías de acceso de archivos supervisados requiere tener en cuenta la sensibilidad de mayúsculas y minúsculas. De lo contrario el grupo no se puede de forma satisfactoria. La solución es crear dos reglas de política de FAM diferentes. Aclaración - Si las series definidas como miembros de un grupo son diferentes sin considerar las mayúsculas y minúsculas, el grupo se puede crear satisfactoriamente. Por ejemplo: 1. C:\ABC 2. C:\abcdef. Si las series definidas como miembros de un grupo son las mismas sin tener en cuenta las mayúsculas y minúsculas, el grupo NO se puede crear. Por ejemplo: 1. C:\ABC 2. C:\abc. Por ello no es necesario especificar miembros con todos los caracteres en mayúsculas o todos en minúsculas. El Creador de grupos no es sensible a las mayúsculas y minúsculas. Sin embargo, en UNIX, que es sensible a las mayúsculas y minúsculas, la vía de acceso /IBM/Guardium es distinta de la vía de acceso /ibm/guardium. Si el usuario desea supervisar ambas vías de acceso, el Creador de grupos actual tiene una limitación y no la verá como la misma vía de acceso.
5. Elija orígenes de datos, acciones y criterios. Sobrescriba los valores que desee cambiar. Pulse Editar para modificar cada campo.
6. Para crear una política nueva e instalarla, pulse Crear e instalar. Para crear la política pero no instalarla, pulse Aceptar.

Tema principal: Reglas y políticas de la actividad de archivos

Supervisar y auditar

Después de identificar los datos confidenciales y de tomar medidas para protegerlos, debe supervisar las actividades que acceden a estos datos. En muchos casos, puede utilizar los datos generados por la supervisión para cumplir con los requisitos de auditoría, ya sean internos o internos.

- Creación de procesos de auditoría
  Racionalizar el proceso de flujo de trabajo de cumplimiento mediante la consolidación, en un lugar, de las siguientes tareas de supervisión de la actividad de base de datos: descubrimiento de activos; asesoramiento y protección de vulnerabilidades; supervisión de actividades de base de datos e informes de auditoría; distribución de informes; aprobación por partes interesadas; y escalados.
- Auditoría e informes
  Guardium organiza los datos que recopila en un conjunto de dominios. Cada dominio contiene un tipo diferente de información relativa a un área específica de interés: acceso a datos, excepciones, infracciones de política, etc.
- Correlación de datos externos
  Este tema describe la creación de tablas personalizadas para la información de empresa que se necesita además de los datos internos de Guardium existentes.
- Conjuntos de privacidad
  Un conjunto de privacidad es un conjunto de elementos que se pueden utilizar para realizar una supervisión especial.
- Alertas personalizadas
  Los mensajes de alerta se pueden distribuir a través de correo electrónico, SNMP, syslog o clases Java™ escritas por el usuario. La última opción se conoce como alerta personalizada.
- Proceso Flat Log
  La opción Flat Log es un proceso para permitir que el dispositivo de Guardium registre información sin analizarla inmediatamente en tiempo real.

- Crear expresión en condición de consulta
  Utilice el icono Añadir expresión, junto a las selecciones Valor, Parámetro, Atributo, para especificar las Condiciones de consulta, incluidas las expresiones matemáticas y las series definidas por el usuario.
- Informes de titularidad de base de datos
  Las revisiones de titularidad son el proceso de validación y garantía de que los usuarios solo tienen los privilegios necesarios para llevar a cabo sus tareas.
- Identificación de usuario
  Guardium proporciona varios métodos para identificar a los usuarios de la aplicación, cuando el usuario de la base de datos no es evidente a partir del tráfico de la base de datos.
- Auditoría de cambio de valores
  La característica Auditoría de cambio de valores realiza un seguimiento de los cambios en los valores de las tablas de base de datos.
- Crear una base de datos de auditoría
  Crear una base de datos de auditoría y realizar actividades de supervisión de cambios de valores.
- Acceso a tablas supervisadas
  Esta característica añade un campo "Última asesorada" a las tablas relevantes, para la interacción con productos de ciclo de vida de datos de Optim Designer.
- Inicio rápido para la supervisión del cumplimiento
  Después de desplegar agentes de supervisión (S-TAP), utilice la herramienta Supervisión del cumplimiento para establecer la supervisión para regulaciones y estándares de seguridad específicos.
- Cómo utilizar PCI/DSS Accelerator para implementar el cumplimiento de PCI
  Configure PCI/DSS Accelerator de IBM Security Guardium's y cree una serie de políticas e informes para cumplir con los requisitos de PCI/DSS.
- Creador de flujos de trabajo
  El Creador de flujos de trabajo se utiliza para definir flujos de trabajo personalizados (pasos, transiciones y acciones) para que se utilicen en el proceso de auditoría.
- Análisis de detección de amenazas
  Guardium incluye un análisis especializado de detección de amenazas que explora y analiza los datos auditados para detectar síntomas que pueden indicar distintos tipos de ataques de base de datos.
- Panel de control de investigación
  El Panel de control de investigación proporciona potentes herramientas para identificar y evaluar problemas que pueden existir en el entorno de Guardium. Utiliza datos sin filtrar locales o de todo el sistema, y proporciona numerosas opciones de filtro para consultar datos en todo un entorno de Guardium, potencialmente desde cualquier recopilador de Guardium dentro de dicho entorno.
- Detección de valores atípicos
  Habilite e inicie la auditoría de detección de valores atípicos en dos pasos sencillos, permitiendo que Guardium haga el trabajo de identificar el comportamiento anormal del usuario y del servidor, y proporcionando una detección temprana de posibles ataques.
- Panel de control de protección de datos
  El panel de control de protección de datos de Guardium proporciona una vista de resumen de los datos de riesgo y cumplimiento destinados a los responsables de seguridad de nivel superior.

Creación de procesos de auditoría

Racionalizar el proceso de flujo de trabajo de cumplimiento mediante la consolidación, en un lugar, de las siguientes tareas de supervisión de la actividad de base de datos: descubrimiento de activos; asesoramiento y protección de vulnerabilidades; supervisión de actividades de base de datos e informes de auditoría; distribución de informes; aprobación por partes interesadas; y escalados.

Automatice e integre las siguientes actividades de auditoría en un flujo de trabajo de cumplimiento:

- La capacidad de agrupar varias tareas de auditoría (informes, asesoramientos de vulnerabilidad, etc.) en un proceso.
- Planifique estos procesos para ejecutarlos de forma regular.
- Ejecute estas tareas en un segundo plano.
- Escriba los resultados de la tarea en un archivo de valores separados por comas (CSV) o en el archivo CEF (ArcSight Common Event Format) y/o reenvíe los resultados a otros sistemas utilizando Syslog.
- Añada comentarios y notaciones.
- Asigne el proceso a su originador para su visualización (el/ella recibirá un nuevo elemento en su lista de tareas pendientes una vez que el resultado esté listo).
- Asigne el proceso para otros usuarios o para un grupo de usuarios o un rol.
- Cree el requisito que estas personas asignadas firman en el resultado.
- Permita el escalado del resultado (asigne a alguien fuera del seguimiento de auditoría original).

Transforme la gestión de seguridad de base de datos de las actividades manuales que requieren mucho tiempo realizadas periódicamente en un proceso continuo automatizado que da soporte a los requisitos de privacidad y gobierno, como por ejemplo PCI-DSS, SOX, Privacidad de datos e HIPAA.

Exporte resultados de auditoría a repositorios externos para un análisis forénsico adicional – Syslog, archivos CSV/CEF, canal de información externo.

El informe Registro del proceso de auditoría muestra un registro de actividades detallado para todas las tareas incluidas las horas de inicio y finalización. Este informe está disponible a los usuarios administradores a través del separador Supervisor de Guardium. Las tareas de auditoría muestran las horas de inicio y de finalización, aunque el inicio y el final de las clasificaciones y los asesoramientos de seguridad (que van a una cola) es el mismo.

Los resultados de cada proceso de flujo de trabajo, incluido la revisión, la aprobación, los seguimientos y los comentarios pueden archivarse y más adelante restaurarse y revisarse a través del centro de investigación.

Un proceso de automatización del flujo de trabajo de cumplimiento responde las siguientes preguntas:

- ¿Qué tipo de informe, asesoramiento, seguimiento de auditoría o clasificación es necesario?
- ¿Quién debe recibir esta información y cómo se manejan las aprobaciones?
- ¿Cuál es la planificación de la entrega?

Entre los elementos adicionales del proceso de automatización del flujo de trabajo de cumplimiento se incluyen:

- Una definición de proceso
- Un plan de distribución, que:
  - Define receptores, que pueden ser usuarios individuales, grupos de usuarios o roles. (Consulte Receptores de proceso).
  - Define la responsabilidad de revisión/firma para cada receptor.
  - Define la secuencia de distribución estableciendo el distintivo Continuo.
- Un conjunto de tareas (consulte Tipos de tareas de proceso)
- Una planificación; el proceso de auditoría puede ejecutarse inmediatamente, o se puede definir una planificación para ejecutar el proceso de forma periódica.

Tipos de tareas de proceso

Un proceso de flujo de trabajo puede contener cualquier número de tareas de auditoría:

- Informes, personalizadas o predefinidas. Guardium proporciona cientos de informes predefinidos, con más de 100 informes específicos de la normativa.
- Informe de asesoramiento de la seguridad. El asesoramiento de la base de datos de seguridad escanea la infraestructura de la base de datos en busca de vulnerabilidades y proporciona un asesoramiento de la salud de la seguridad de los datos y de la base de datos, con medidas históricas y en tiempo real. Compara el entorno actual con las pruebas de vulnerabilidad preconfiguradas basadas en deficiencias y vulnerabilidades conocidas, agrupadas utilizando métodos recomendados de seguridad de base de datos comunes (como STIG y CIG1), además de incorporar pruebas personalizadas. La aplicación genera una Tarjeta de informe de salud de seguridad, con métricas ponderadas (basadas en las prácticas recomendadas) y recomienda planes de acción para ayudar a reforzar la seguridad de la base de datos.
- Un seguimiento de auditoría de entidad. Se produce un informe detallado de la actividad relacionada con una entidad específica (por ejemplo, una dirección IP de cliente o un grupo de direcciones).
- Un conjunto de privacidad. Un informe que detalla el acceso a un grupo de pares de campos de objetos (por ejemplo, un número de seguridad social y una fecha de nacimiento) se genera durante un periodo de tiempo específico.
- Un proceso de clasificación. Los datos y los metadatos de base de datos existentes se exploran, informando sobre la información que puede ser confidencial, como números de seguridad social o números de tarjeta de crédito.
- Un canal de información externo. Los datos se pueden exportar a una aplicación especializada externa para obtener un análisis forense más detallado.
  Nota: El canal de información de datos externos opcionales es un componente opcional habilitado por la clave del producto. Si esta característica no se ha habilitado, esta opción no aparecerá en la selección de Tarea de auditoría y la lista Tipo de canal de información estará vacía.

Procesos de flujo de trabajo, Gestión central y Agregación

En un Gestor central, los informes pueden hacer referencia a datos de orígenes de datos remotos (unidades gestionadas). Los procesos de auditoría que utilizan estos informes solo serán accesibles desde el Gestor central y no serán visibles desde las unidades gestionadas.

La automatización de flujo de trabajo (proceso de auditoría) para el servidor Agregador ahora incluye la posibilidad de crear bases de datos ad-hoc para cada tarea de agregador y especificar solo los días relevantes para esa tarea.

Nota: Las bases de datos ad-hoc para el servidor de agregación pueden conservarse en el sistema hasta 14 días (en función del valor del mandato de CLI, drop_ad_hoc_audit_db) para un análisis posterior a la ejecución por parte de los servicios de soporte de Guardium.

Cuando se definen informes en el proceso de auditoría, el número de días del informe (definido por los campos DESDE-HASTA) no debe superar un determinado umbral (un mes de forma predeterminada). Si se supera este umbral, se producirá un error de tiempo de ejecución cuando se intente ejecutar la tarea de auditoría en el agregador.

Está permitido crear una tarea de auditoría con un rango DESDE-HASTA que es más ancho que el valor max_audit_reporting (establecido en CLI) porque los procesos de auditoría definidos en el agregador pueden ejecutarse en recopiladores gestionados (cuando este agregador es un gestor). Las tareas de auditoría se ejecutan en una unidad de recopilador, no tiene una limitación de max_audit_reporting.

Por lo tanto, es válido guardar tareas más allá del rango permitido, pero obtendrá una excepción de tiempo de ejecución cuando la tarea se ejecute en el agregador.

El umbral del informe de auditoría se puede configurar utilizando el mandato de CLI, show max_audit_reporting o store max_audit_reporting. No hay ningún mensaje de aviso cuando se crea un informe con un rango DESDE-HASTA no válido. En su lugar, aparece un mensaje fijo en el panel Parámetros de tarea de la pantalla del menú de configuración del proceso de auditoría (Herramientas/Creador de procesos de auditoría. abra las Tareas de auditoría para visualizar los parámetros de tarea). El mensaje fijo es:

```
En los agregadores, sólo se ejecutarán los informes que no superen el rango de tiempo permitido (CLI: max_audit_reporting).
```

Nota: Cuando se ejecuta una instalación de parches, se detienen todos los procesos de auditoría.

Detener un proceso de auditoría

La detención de un proceso de auditoría solo se puede realizar si las tareas de auditoría no se han ejecutado o están en ejecución. Al detenerse un proceso de auditoría no se ejecutará ninguna tarea más que no se haya iniciado. La detención de un proceso de auditoría no produce resultados parciales. El proceso de auditoría se detiene y el resultado es un mensaje de error detenido. Sin embargo, si las tareas se completan, la detención de un proceso de auditoría no detendrá el envío de los resultados.

Detenga un proceso de auditoría utilizando la invocación GuardAPI (coloque el cursor en cualquier línea y efectúe una doble pulsación para obtener más detalles) en el informe Cumplir > Herramientas y vistas > Informe de proceso de auditoría.

Para cualquier usuario, al detener un proceso de auditoría se mostrará solo la línea que pertenece a dicho usuario (solo las tareas, no todos los detalles). Un usuario administrador puede ver todos los detalles y puede detener los procesos de auditoría de cualquiera. Un usuario solo puede detener sus propios procesos de auditoría.

Nota:

Las consultas que utilizan un origen remoto no se pueden detener. Los informes en línea que utilizan un origen remoto no se pueden detener.

La detención de procesos de auditoría no se aplica a las tareas de auditoría de conjuntos de privacidad ni a las tareas de auditoría de canal de información externo. Si las tareas de Conjunto de privacidad o Canal de información externo se han iniciado, finalizarán aunque el proceso se haya detenido.

Distribución de resultados

Se notificará a los destinatarios del proceso de auditoría a través del correo electrónico y/o su lista de tareas pendientes de los resultados del proceso de auditoría. Puede designar cualquier receptor como un firmante para un proceso, en cuyo caso los resultados se pueden mantener opcionalmente en ese punto de la lista de distribución, hasta que el receptor firme electrónicamente los resultados o los libere. Los receptores pueden ser usuarios individuales, grupos de usuarios o roles.

Resumen de proceso de auditoría

En la pantalla Buscador de procesos de auditoría está el Resumen del estado del proceso de auditoría. Esta sección contiene información sobre los procesos de auditoría planificados, así como los resultados, los receptores pendientes y los errores. Este resumen es una consolidación de datos de varios informes de proceso de auditoría.

También hay un botón para suprimir los resultados del proceso de auditoría. Consulte la pantalla Buscador de procesos de auditoría. Busque el botón Resultados, junto al botón Ejecutar una vez ahora (opciones de Ver o Suprimir).

Suprima los resultados del proceso de auditoría, pero realice el seguimiento o registre quién suprimió el informe. El rol audit-delete se utiliza para realizar el seguimiento o registrar cuando se ha suprimido un resultado del proceso de auditoría. Los usuarios con el rol audit-delete pueden suprimir informes. Los usuarios administrativos también pueden suprimir informes. El seguimiento se realiza mediante el informe Seguimiento de auditoría de actividad de usuario.

Nota: Los resultados del proceso de auditoría de orígenes remotos están limitados a 100.000 resultados. Para ir más allá de ese límite, utilice el mandato de CLI, store save_result_fetch_size (show save_result_fetch_size).

Receptores de proceso

Puede definir cualquier número de receptores para un proceso de automatización de flujos de trabajo y puede controlar el orden en el que reciben los resultados. Además, los receptores pueden notificar a receptores adicionales, utilizando la función Escalar. También es posible ejecutar un proceso de auditoría sin ningún receptor definido. Por ejemplo, un proceso de auditoría sin receptores que escriba en syslog y que no tenga necesidad de revisar (o firmar) los resultados.

¿Quién puede ser un receptor?

En el panel Definición de proceso, la lista desplegable de receptores incluye todos los usuarios, grupos de usuarios y roles de Guardium (los grupos y los roles se etiquetan como tales). Cuando se selecciona un grupo o un rol, todos los usuarios que pertenecen al grupo o que tienen ese rol recibirán los resultados.

Si se selecciona un receptor de grupo y alguna tarea de automatización de flujo de trabajo utiliza el parámetro de tiempo de ejecución especial ./LoggedUser en una condición de consulta, la consulta se ejecutará por separado para cada usuario en el grupo y cada usuario recibirá solo sus resultados.

Por ejemplo, suponga que su empresa tiene tres DBA y cada DBA está a cargo de un conjunto distinto de servidores. Utilizando el recurso Subida de datos personalizados suba las áreas de responsabilidades de cada DBA (con las IP de servidor) al sistema Guardium y correlaciónelo con el dominio de actividad de base de datos y, a continuación, utilice un informe en este dominio personalizado como una tarea de auditoría. Si un grupo de usuarios que contiene los tres DBA se ha designado como el receptor, cada DBA solo recibirá el informe relevante para su conjunto de servidores.

Si se selecciona un receptor de grupo y es necesario finalizar la sesión, cada miembro del grupo debe firmar los resultados por separado (como se ha explicado anteriormente, cada miembro del grupo puede estar examinando un conjunto de resultados diferente).

Un receptor puede ser únicamente una dirección de correo electrónico y los resultados se enviarán a esa dirección de correo electrónico. Al especificar una dirección de correo electrónico, se solicitará al usuario que especifique un usuario que se utilizará para filtrar los datos. El usuario debe ser el mismo usuario que ha iniciado la sesión o un usuario bajo el usuario que ha iniciado sesión en la jerarquía de datos.

Si se selecciona un receptor de rol, solo un usuario con ese rol necesitará firmar los resultados y se notificará a otros usuarios con dicho rol cuando se hayan firmado los resultados.

Nota:

Cuando se crea un suceso de flujo de trabajo, a todos los estados utilizados por dicho suceso se les puede asignar un rol (lo que significa que los sucesos sólo pueden ser vistos por este rol cuando estén en este estado). Cuando se asigna un suceso a un proceso de auditoría, es importante que cada rol que se asigne a un estado de este suceso tenga un receptor en este proceso de auditoría. De lo contrario, es posible que una fila de resultado de auditoría pueda colocarse en un estado en el que ninguno de sus receptores pueda ver esta fila o cambiar su estado.

Si esto va a suceder, el usuario administrativo (que puede ver todos los sucesos, independientemente de sus roles) podría ver la fila y cambiar su estado. Sin embargo, si la seguridad a nivel de datos está activada, es posible que el usuario administrador no pueda ver esta fila. El usuario administrativo tendría que desactivar la seguridad a nivel de datos (desde el perfil global) o tener el rol dataset_exempt. Es importante configurar el proceso de auditoría para que todos los roles que deban actuar en un suceso asociado a este proceso de auditoría sean receptores de este proceso de auditoría.

Notificación por correo electrónico

De forma opcional, se puede notificar a los receptores acerca de los nuevos resultados del proceso mediante correo electrónico y existen dos opciones para distribuir resultados por correo electrónico:

- Sólo enlace: La notificación de correo electrónico contendrá un enlace de hipertexto a los resultados almacenados en el sistema Guardium. Para que un enlace funcione, debe acceder al correo desde un sistema que tenga acceso al sistema Guardium. Consulte la siguiente sección para obtener más información sobre los enlaces de correo electrónico.
- Resultados completos: Un archivo PDF o un archivo CSV generado que contenga los resultados se adjuntará al correo electrónico, excepto para un escalado que especifique un receptor que no esté incluido en la lista de distribución original, en cuyo caso no se adjuntará ningún archivo PDF o CSV. Cuando se selecciona la opción Resultados completos, se debe tener cuidado, ya que se pueden incluir en el archivo PDF o CSV datos confidenciales y privados. Cuando se ejecuta un proceso de auditoría, si hay un receptor con Resultados completos con CSV seleccionado, no genera archivos CSV para las tareas de tipo Asesoramiento, Clasificador o Canal de información externo. Estos tipos de tareas tampoco pueden generar archivos CSV/CEF/PDF para exportar. Sólo para las tareas de tipo Informe, Conjunto de privacidad o Seguimientos de auditoría de entidad, y si hay un receptor con Resultados completos en CSV seleccionado, se generarán archivos CSV.
  Nota: Al visualizar resultados de auditoría, si ya existe un PDF generado, aparecerá un botón Recrear PDF para que el usuario vuelva a crear y descargar el PDF regenerado.

Enlaces de hipertexto para procesar resultados

En los mensajes de correo electrónico, hay condiciones donde los enlaces para procesar resultados en el sistema Guardium no funcionarán. Por ejemplo:

- Si está accediendo al correo electrónico desde una ubicación desde la que normalmente no puede acceder al sistema Guardium, los enlaces no funcionarán. Por ejemplo, cuando está fuera de la oficina, es posible que tenga acceso a su correo electrónico a través de Internet, pero no a la LAN o red privada de la empresa, donde está instalado el sistema.
- Si no ha accedido a su correo electrónico durante un periodo de tiempo que supera el tiempo que se mantienen los resultados del informe, estos resultados no estarán disponibles cuando pulse el enlace. Por ejemplo, si los resultados se conservan durante siete días, pero ha estado en vacaciones durante dos semanas, es posible que el correo electrónico contenga enlaces a resultados con una antigüedad superior a siete días y esos enlaces no funcionarán.

Acerca de los enlaces de receptores bloqueados

Una vez que se ha ejecutado un proceso, la lista de receptores existente queda bloqueada, lo que significa:

- No puede suprimir receptores de la lista.

- No puede subir o bajar receptores existentes en la lista.
- Puede añadir receptores a final de la lista en cualquier momento, y volver a poner los nuevos receptores en ese momento.
- Si se suprime la cuenta de usuario de Guardium para un receptor de la lista, la cuenta de usuario administrador (que nunca se suprime) se sustituye por ese receptor. De este modo, el usuario administrador recibe todas las notificaciones de correo electrónico que se han enviado a un receptor suprimido, y el usuario administrador debe actuar en función de los resultados que se hayan enviado a ese receptor.
- Si necesita crear un conjunto de receptores totalmente diferente para un proceso existente, desactive el proceso original, cree un clon de mismo y, a continuación, realice las modificaciones en la lista de receptores de la versión clonada antes de guardarla.

Cómo se suministran los resultados a los receptores

Los resultados se suministran a los usuarios de Guardium listados en la lista de receptores, sujeto al recuadro de selección Continuo, tal como se indica a continuación:

- Si el recuadro de selección Continuo está marcado, la distribución continua al siguiente receptor de la lista sin interrupción.
- Si el recuadro de selección Continuo no está marcado, la distribución al siguiente receptor se retiene hasta que el receptor actual realiza la acción necesaria (revisar o firmar).

Por ejemplo, suponga que desea definir un proceso de flujo de trabajo de la siguiente manera:

- DBA: Todos los DBA deben recibir sus resultados al mismo tiempo, con cada DBA recibiendo un conjunto de resultados diferente basado en las IP de servidor asociadas al mismo.
- Solo cuando todos los DBA hayan firmado, el Gestor de DBA debe ver los resultados
- Solo cuando el Gestor de DBA entrega el informe, los auditores deben ver los resultados
- Todos los auditores deben recibir los informes al mismo tiempo, pero solo uno de ellos (cualquiera de ellos) tiene que firmar cada resultado. Se notificará a los demás cuando se firme un resultado.
- Un auditor puede escalar un resultado en el Gestor de auditoría.

Para definir este flujo:

- El grupo de DBA se denominará como el primer receptor
- El gestor de DBA sería el siguiente en la lista.
- El rol de auditores (no grupo) sería el siguiente en la lista. Cualquier auditor podría firmar y los demás serán notificados. Además, cualquier auditor puede escalar un conjunto de resultados al gestor de auditoría.
  Nota: Los resultados se distribuirán solo al siguiente receptor cuando el receptor actual haya marcado el botón Continuo. Esto es completamente independiente de la funcionalidad de revisión/firma y no depende de la funcionalidad de revisión/firma.
  Nota: Los resultados del proceso que se exportan a archivos CSV o CEF se envían a otra ubicación de red mediante el mecanismo de exportación y archivado de Guardium. Estos resultados no están sujetos a la lista de receptores ni a ninguna acción de firma. Están sujetos a la planificación de exportación de CSV/CEF de Guardium (si se ha definido alguna) y están sujetos a los permisos de acceso que se han otorgado para el directorio en el que finalmente se han almacenado.

Exportación de salidas de tareas de auditoría a archivos CSV, CEF o PDF

Los informes que contienen información que pueden ser utilizados por otras aplicaciones, o informes que contienen grandes cantidades de datos, se pueden exportar a otros formatos de archivo. La salida de las tareas Informe, Seguimiento de auditoría de entidad y Conjunto de privacidad se puede exportar a archivos CSV (valor separado por comas) y (valores separados por comas), y la salida de los informes de actividad de base de datos se puede exportar a un archivo CEF (Common Event Format) de ArcSight.

Además, la salida del archivo CEF y CSV se puede grabar en syslog. Si se utiliza la capacidad de syslog remota, esto resultará en el reenvío inmediato del archivo CEF/CSV de salida a las ubicaciones de syslog remotas. La función syslog remota proporciona la capacidad de direccionar mensajes desde cada combinación de recurso y gravedad a un sistema remoto específico. Consulte la descripción del mandato de CLI remotelog (syslog) CLI para obtener más información.

Cada registro en el archivo CSV o CEF representa una fila en el informe.

El archivo exportado se crea además de la salida de tarea estándar, no lo sustituye. Estos archivos son útiles cuando necesita:

- Integrarse con un SIEM existente (Security Incident and Event Manager) en su infraestructura (Qradar, ArcSight, Network Intelligence, LogLogic, TSIEM, etc.) .
- Revisar y analizar conjuntos de resultados de tareas de conformidad muy grandes. (Los conjuntos de resultados de tareas que están pensados para la presentación web están limitados a 5.000 filas de salida, mientras que no hay ningún límite en el número de filas que se escribirán en un archivo CEF o CSV exportado).

Los archivos CSV y CEF exportados se almacenan en el sistema Guardium y se denominan en el formato:

```
proceso_tarea_AAAA_MMM_DD-HHMMSS.<csv | cef>
```

Donde proceso es una etiqueta que define en la definición de proceso de auditoría, tarea es una etiqueta de segundo nivel que puede definir para cada tarea dentro del proceso y AAAA_MMM_DD-HHMMSS es una indicación de fecha y hora creada cuando se ejecuta la tarea.

No puede acceder a los archivos CSV o CEF exportados directamente en el sistema Guardium. El administrador de Guardium debe utilizar la función de exportación CSV/CEF para mover estos archivos desde el sistema Guardium a otra ubicación de la red. Para acceder a estos archivos, consulte con el administrador de Guardium para determinar la ubicación en la que se han copiado.

El hecho de que los archivos exportados se envíen fuera del sistema Guardium tiene dos implicaciones importantes:

- El release de estos archivos no está conectado al plan de distribución de resultados definido para el proceso de auditoría. Estos archivos se exportan según una planificación definida por el administrador de Guardium.
- Una vez que se ejecuta la función de exportación de CSV/CEF, todos los archivos exportados estarán disponibles para cualquier usuario (sea o no usuario de Guardium) que pueda acceder al directorio de destino definido para la operación de exportación de CSV/CEF. Por esta razón, es posible que el administrador de Guardium desee planificar trabajos adicionales (fuera del sistema Guardium) para copiar conjuntos de archivos exportados del directorio de destino de exportación de CSV/CEF de Guardium en los directorios con permisos de acceso adecuados.

La actividad de exportación de CSV/CEF está disponible en el informe de actividad de agregación/archivado.

Nota: Si se ha habilitado la seguridad a nivel de datos observados, entonces se filtrará la salida del proceso de auditoría (incluidos archivos) de forma que los usuarios solo verán información sobre sus bases de datos asignadas. Los archivos enviados a un receptor de correo electrónico como un archivo adjunto se filtrarán. Sin embargo, los archivos que se han descargado localmente en la máquina y que luego se han trasladado a otro lugar utilizando la función de exportación de resultados no están sujetos al filtrado de seguridad a nivel de datos. Consulte Exportación de CSV/CEF más adelante en este tema para obtener más información sobre la exportación de CSV/CEF.

En la tabla siguiente se resume lo que sucede al exportar un archivo de proceso de auditoría a CSV/CEF/PDF.

Tabla 1. Exportación de salidas de tareas de auditoría a archivos CSV, CEF o PDF

Función	Nivel	CSV	CEF	PDF
Adjuntar a correo electrónico	Receptor	Botón de selección Detalles completos --> Recuadro de selección PDF	N/D	Botón de selección Detalles completos --> Recuadro de selección PDF Los botones de selección solamente son para el PDF de receptor
Exportar archivo	Tarea	Recuadro de selección Exportar archivo CSV	Recuadro de selección Exportar archivo CSV	Recuadro de selección Exportar archivo CSV
Informe vacío y Aprobar si está vacío = sí	Receptor	Exportación no afectada (se exportarán los archivos vacíos) Archivo adjunto, sin archivo adjunto de correo electrónico	Exportación no afectada (se exportarán los archivos vacíos) Archivo adjunto, sin archivo adjunto de correo electrónico	Exportación no afectada (se exportarán los archivos vacíos) Archivo adjunto, sin archivo adjunto de correo electrónico
Comprimir archivo adjunto	Proceso de auditoría	Si no se ha generado ningún archivo, no hay nada que comprimir Fusionar todos los CSV en un archivo ZIP	N/D	Si no se ha generado ningún archivo, no hay nada que comprimir PDF no se ha comprimido
Comprimir (exportar)	Tarea	Archivo comprimido y separado para cada archivo CSV	Archivo comprimido y separado para cada archivo CSV	PDF no comprimido

Cómo funciona Comprimir para enviar por correo electrónico y Comprimir para la salida de tareas de auditoría

Comprimir para enviar por correo electrónico es el nivel de control más alto para Exportar tarea de auditoría. Comprimir para enviar por correo electrónico produce un conjunto de archivos CSV o CEF. PDF nunca se comprime.

La compresión funciona en archivos individuales.

Nota: Para los archivos adjuntos CVS, cuando se deselecciona Comprimir CVS por correo electrónico, Comprimir puede seguir aplicándose. Y Comprimir puede ser por tarea. Por tanto, una tarea de auditoría puede enviar un archivo .csv mientras que otra puede enviar un archivo .csv.gz, en el mismo correo electrónico.

La interacción de Comprimir CVS por correo electrónico y Comprimir es la siguiente:

- Con Comprimir CVS por correo electrónico seleccionado (independientemente de si Comprimir también está seleccionado), el archivo adjunto es un archivo comprimido de archivos CSV.
- Con Comprimir CVS por correo electrónico no seleccionado y Comprimir seleccionado, el archivo adjunto es un conjunto de archivos csv.gz.
- Con Comprimir CVS por correo electrónico no seleccionado y Comprimir no seleccionado, el archivo adjunto es un conjunto de archivos csv.
- Con Comprimir seleccionado, Bajar todo será csv.gz.
- Con Comprimir deseleccionado, Bajar todo será csv.
- Con Comprimir seleccionado o deseleccionado, Bajar visualizados seguirá siendo csv.
- Con Comprimir seleccionado, la exportación de archivos CSV/CEF será gzipped.
- Con Comprimir deseleccionado, la exportación de archivos CSV/CEF no será gzipped.

Exportar a SCAP o AXIS

En la Definición del proceso de auditoría, en la sección Añadir tarea nueva, al seleccionar un Tipo de tarea de Asesoramiento de seguridad, aparecerán distintas opciones: Exportar AXIS xml y Exportar SCAP xml. Elija una de estas selecciones para poder guardar los resultados del proceso de auditoría y para transferir el archivo XML al destino configurado para la exportación de resultados (Gestionar > Gestión de datos > Exportación de resultados (Archivos)). Las opciones adicionales son para configurar el formato PDF: Informe, Diferencias, Informe y diferencias.

SCAP es Security Content Automation Protocol. AXIS es Apache EXtensible Interaction System y lo utiliza QRadar.

Creación o cambio de informes

Utilice el Creador de informes para crear o personalizar informes, incluida la personalización como, por ejemplo, aplicar colores de resaltado a filas. Para abrir el Creador de informes, vaya a Informes > Herramientas de configuración de informes > Creador de informes.

Crear un proceso de flujo de trabajo de auditoría

1. Abra el Creador de procesos de auditoría navegando a Cumplir > Herramientas y vistas > Creador de procesos de auditoría.
2. Pulse el botón Nuevo para abrir el panel Definición de proceso de auditoría. El panel Definición de proceso de auditoría se divide en tres secciones: General, Receptores y Tareas.
3. Vaya primero a la sección Tareas. Debe definir al menos una tarea de auditoría para poder guardar el proceso. Establezca opciones en cada tarea. Realice el procedimiento adecuado para cada tarea de auditoría que desee incluir en el proceso de auditoría. Las opciones de tareas que se detallan en esta sección son:
    - Definir una tarea de informe
    - Definir una tarea de asesoramiento de seguridad
    - Definir una tarea de seguimiento de auditoría de entidad
    - Definir una tarea de conjunto de privacidad
    - Definir una tarea de proceso de clasificación
    - Definir una tarea de canal de información externo
4. Vaya a la sección Receptores. Abra el recuadro desplegable y añada los receptores para el proceso. Consulte Añadir receptores. Son necesarias marcas de verificación para determinar la acción necesaria, adiciones a la lista de tareas pendiente, la notificación a través de notificaciones de correo electrónico y la distribución continua. De nuevo, consulte el apartado Añadir receptores para obtener información completa sobre cómo establecer estas opciones.
5. Vaya a la sección General. Especifique un nombre en el recuadro Descripción. No incluya caracteres de apóstrofo.
6. Marque el recuadro Activo para asociar una planificación a este proceso.

7. Marque el recuadro Resultados del archivado si desea almacenar los resultados fuera de línea una vez que haya caducado el periodo de retención. Cuando los resultados se han archivado, puede restaurarlos en el sistema para volver a visualizarlos más adelante.
8. Utilice el recuadro Archivar depuración de resultados antes de la revisión para suprimir los resultados de un proceso adhoc sin retención hasta que todos los revisores hayan revisado, se hayan realizado todas las aprobaciones y se hayan atendido todas las actividades. Esta característica proporciona al usuario una opción de supresión de resultados en un periodo de tiempo especificado (por ejemplo, 1 día) tanto si los resultados se han revisado como si no.
9. En los recuadros Mantener durante un mínimo de (n) días o (n) ejecuciones, especifique cuánto tiempo mantener los resultados, ya sea un número de días (0 de forma predeterminada) o un número de ejecuciones (5 de forma predeterminada). Después de esto, los resultados se archivarán (si se marca el recuadro Mantener durante un mínimo de) y se depurarán del sistema.
   Nota: Los resultados sólo se mostrarán si hay receptores para los resultados. Añada receptores, vuelva a ejecutar los resultados y la ejecución se mostrará ahora en la lista desplegable.
10. Si una o más tareas crean archivos CSV o CEF, también puede especificar una etiqueta para que se incluya en todos los nombres de archivo, en el recuadro Etiqueta de archivo CSV/CEF. Estos archivos también se pueden comprimir, o incluirse en un zip, pulsando en el recuadro Comprimir CVS por correo electrónico para añadir una marca de selección.
    Nota: Existe un límite en la exportación de tamaños de archivo de CSV/CEF superiores a 10240 MB (10.240 GB). Como práctica recomendada se recomienda marcar el recuadro Comprimir CVS por correo electrónico.
11. El campo Asunto de correo electrónico en la Definición del proceso de auditoría se utiliza en los correos electrónicos para todos los receptores para ese proceso de auditoría. El sujeto puede contener una (o varias) de las variables siguientes que se sustituirán en el tiempo de ejecución para el asunto:
    - %% ProcessName se sustituirá por la descripción del proceso de auditoría
    - %% ExecutionStart se sustituirá por la fecha y la hora de inicio de la primera tarea.
    - %% ExecutionEnd se sustituirá por la fecha y hora de finalización de la última tarea.

    Después de especificar un asunto, comprobará si hay alguna variable (empezando por%% presente) y garantizará que todas sean variables válidas.

12. Opcionalmente, asigne roles de seguridad.
13. Opcionalmente añada comentarios.
14. Pulse los botones adecuados para planificar o ejecutar un proceso de flujo de trabajo de auditoría.
15. Pulse Guardar. No deje esta pantalla de menú para realizar otra configuración antes de guardar el trabajo. El trabajo en curso no se guarda y no se mantiene en suspensión creada a medias si deja esta sección para crear algo más que sea necesario para la tarea de auditoría.

    Por ejemplo, para definir una tarea de asesoramiento en el Creador de procesos de auditoría, primero es necesario ir al Creador de asesoramientos de seguridad para crear pruebas de asesoramiento y, a continuación, a Definiciones de orígenes de datos para identificar las bases de datos que deben asesorarse. Guarde el trabajo al crear el flujo de trabajo de auditoría y, a continuación, vaya a otras tareas o realice primero esas otras tareas y, a continuación, cree el proceso de flujo de trabajo de auditoría.

Añadir receptores

1. En la columna Receptor, seleccione un receptor en la lista desplegable de usuarios, grupos o roles de Guardium individuales. Si selecciona un grupo o un rol, todos los miembros del grupo o los usuarios con ese rol recibirán los resultados; y si la firma es necesaria, solo es necesario que firme los resultados un miembro o un usuario.
2. En la columna Acción necesaria, seleccione una opción:
   - Revisar (el valor predeterminado): Indica que este receptor no necesita firmar los resultados.
   - Revisar y firmar: Indica que este receptor debe firmar los resultados (electrónicamente, pulsando el botón Firmar resultados al visualizar los resultados en línea).
3. En la columna Lista de tareas pendientes, marque o quite la marca del recuadro de selección Añadir para indicar si se debe notificar a este receptor los resultados pendientes en la lista de tareas pendientes del proceso de auditoría.
   Nota: Para enviar archivos a un servidor externo sin enviar un correo electrónico y sin añadir resultados a la lista de tareas pendientes, defina un proceso de auditoría sin receptores. Asimismo, desmarque el recuadro de selección de lista de tareas pendientes en la sección Añadir receptor y elimine/no añada ningún receptor en la sección del receptor para no añadir resultados a la lista de tareas pendientes.
4. En la columna Notificación por correo electrónico, seleccione una opción:
   - No: No se enviará ningún correo electrónico al receptor.
   - Sólo enlace: El correo electrónico contendrá un enlace de hipertexto a los resultados (en el sistema Guardium).
   - Resultados: El correo electrónico contendrá una copia de los resultados en formato PDF o CSV. Tenga en cuenta que los resultados de las tareas de Clasificación o Asesoramiento pueden devolver información confidencial.
5. El recuadro de selección de la columna Continuo controla si la distribución de los resultados continúa o no en el siguiente receptor (el valor predeterminado) o se detiene hasta que este receptor ha realizado la acción adecuada. Si el recuadro Continuo se desmarca y el receptor es un grupo o un rol, cuando cualquier usuario que es un miembro o ese grupo o rol lleva a cabo la acción seleccionada, los resultados se entregarán al siguiente receptor en la lista.
   Nota: Los resultados se distribuirán solo al siguiente receptor cuando el receptor actual haya marcado el botón Continuo. Esto es completamente independiente de la funcionalidad de revisión/firma y no depende de la funcionalidad de revisión/firma.
6. Pulse Añadir para añadir el receptor al final de la lista y repita estos pasos para cada receptor. Se requiere un receptor.
7. Los receptores que no son usuarios están permitidos. Seleccione: Correo electrónico y, a continuación, especifique una dirección de correo electrónico, y los resultados se enviarán a esa dirección de correo electrónico. Al entrar una dirección de correo electrónico que no sea de usuario, existe un requisito de que un nombre de usuario se utilizará para filtrar los datos. El usuario debe ser el mismo usuario que ha iniciado la sesión o un usuario bajo el usuario que se ha registrado en la jerarquía. Este usuario se guardará en una nueva columna en la sección Receptores de la pantalla.
8. Aprobar si está vacío: Cuando este recuadro de selección está seleccionado, si todos los informes de la tarea están vacíos, se hará lo siguiente: firmar automáticamente el resultado (y/o marcarlo como visualizado); pulsar automáticamente Continuar (si es relevante); no se enviará el correo electrónico de notificación; no se añadirá la tarea a la lista de tareas pendientes de ese usuario; no se generará ningún archivo PDF/CSV/CEF. Con este recuadro de selección, los resultados de auditoría vacíos se firmarán automáticamente y los resultados seguirán pareciéndose a cualquier otro resultado de auditoría completo (visualizado/firmado) cuando se examinan los registros de resultados de auditoría. Esta acción se aplicará a los informes vacíos y a los resultados de asesoramiento de seguridad vacíos. Consulte la tabla que resume lo que sucede cuando Aprobar si está vacío = Sí en la sección Exportación de salidas de tareas a archivos CSV, CEF o PDF.

Exportar a un archivo CSV o CEF

La salidas de tareas de auditoría Informe, Seguimiento de auditoría de entidad y Conjunto de privacidad puede exportarse a archivos CSV y la salida de tarea de auditoría Informe puede exportarse a un archivo CEF. En la sección Informe, Seguimiento de auditoría de entidad o Conjunto de privacidad bajo Tareas de auditoría, haga lo siguiente:

1. Seleccione un título.
2. Especifique una etiqueta opcional para el archivo en el recuadro Etiqueta de archivo CSV/CEF. El valor predeterminado procede de la Descripción de la tarea. Esta etiqueta será un componente del nombre de archivo generado (otro será la etiqueta definida para el proceso de automatización de flujo de trabajo).

3. Marque Exportar archivo CSV o Exportar archivo CEF.
   Nota: La salida del archivo CEF solo es adecuada para los informes de dominio de acceso a datos (por ejemplo, Acceso, Excepciones o Infracciones de política). Otros dominios como los dominios de autosupervisión de Guardium (Agregación/Archivado, Proceso de auditoría, Inicios de sesión de Guardium, etc.) no se correlacionan con extensiones CEF.
4. Si se ha seleccionado Exportar archivo CEF, opcionalmente marque el recuadro Escribir CEF en Syslog para escribir los registros CEF en syslog. Si el recurso de syslog remoto está habilitado, los registros del archivo CEF se grabarán en el syslog remoto.
5. Si se selecciona el recuadro Comprimir, se comprimirán los archivos CSV/CEF que se van a exportar.
6. Si se selecciona el recuadro Exportar archivo PDF, se crea y se exporta un archivo PDF (con un nombre similar al archivo de exportación CSV) para esta tarea de auditoría y se exporta junto con los archivos CSV/CEF.
   Nota: El archivo PDF de exportación no se comprimirá, incluso si se ha seleccionado el recuadro Comprimir del paso anterior.

Definir una tarea de informe

Si aún no ha empezado a definir un proceso de automatización del flujo de trabajo de cumplimiento, cree un proceso de flujo de trabajo antes de realizar este procedimiento. Si el informe que se va a utilizar todavía no se ha definido, hágalo primero.

1. Si el panel Añadir tarea nueva no está abierto, pulse Añadir la tarea de auditoría.
2. Pulse el botón de selección Informe.
3. Hay varias opciones para Etiqueta de archivo CSV/CEF, Exportar CSV/CEF, Exportar PDF, Escribir en Syslog y Comprimir. Consulte Exportar a un archivo CSV o CEF.
4. La selección de Opciones de PDF son: Informe (los resultados actuales), Diferencias (diferencias entre un informe anterior y un informe nuevo) e Informe y diferencia (ambos).
   Nota: La selección de Opciones de PDF se aplica a los archivos adjuntos PDF y los archivos de exportación PDF. El resultado Diferencias solo se aplica después de la primera vez de ejecutar esta tarea. No hay Diferencias con un resultado anterior si no hay ningún resultado anterior. El número máximo de filas que se pueden comparar a la vez es de 5000. Si el número de filas de resultado sobrepasa el máximo, el mensaje

   ```
   (primero comparar solo 5000 filas)
   ```

   aparecerá en el resultado de diferencias.
5. Especifique todos los valores de parámetro en el panel Parámetros de tarea. Los parámetros variarán en función del informe seleccionado.
6. Pulse Aplicar.

API para la ejecución automática

De forma predeterminada, la aplicación Guardium se proporciona con datos de configuración que enlazan muchas de las funciones de la API con informes, proporcionando a los usuarios, a través de la GUI, llamadas preparadas a las API a partir de datos de informes. Utilice la Asignación de API en Informes para enlazar funciones API adicionales con informes de Guardium predefinidos o informes personalizados. La API de opción de menú para la ejecución automática aparecerá en Añadir la tarea de auditoría: Informe al seleccionar un informe de Guardium predefinido o un informe personalizado que tenga campos en el informe que estén enlazados a parámetros de API. Ejemplos de informes predefinidos en los que aparecerán la API para la opción de menú de ejecución automática son Infracciones de política de acceso, Bases de datos descubiertas y Detalles de grupo de Guardium.

Creador de flujos de trabajo

La secuencia formal de tipos de sucesos creados en el Creador de flujos de trabajo se gestiona pulsando en el botón Suceso y columnas adicionales en la ventana Tareas de auditoría. Este botón aparecerá después de que se haya creado y guardado una tarea de auditoría. Este botón adicional no aparecerá hasta que se guarde la tarea de auditoría. Configure estas actividades de flujo de trabajo al añadir una tarea de auditoría:

1. Cree y guarde una tarea de auditoría. Después de guardar, aparecerá un botón adicional, Sucesos y columnas adicionales.
2. Pulse este botón adicional.
3. En la siguiente pantalla, ponga una marca de selección en el recuadro para Suceso y aprobación. El flujo de trabajo creado en Creador de flujos de trabajo aparecerá como una opción en Suceso y aprobación.
4. Resalte esta opción. Aplique (guarde) su selección.
5. Si es necesaria información adicional (como códigos de empresa, etiquetas de unidades de negocio, etc.) como parte del informe de flujo de trabajo, añada esta información en la sección Columna adicional de la pantalla y luego pulse Aplicar (guardar). Para seleccionar la columna de grupos predefinidos o creados, cambie la columna Tipo por Grupo. Cuando haya terminado, cierre esta ventana.
6. Aplique (guarde) su tarea de auditoría. Aplique (guarde) toda la definición del proceso de auditoría.

Este botón Suceso y columnas adicionales aparecerá en todas las tareas de auditoría. Al situar el cursor sobre este botón, aparecerá un globo de información indicando al usuario si la tarea de auditoría tiene suceso o una columna de aprobación enlazada a la tarea de auditoría específica.

Nota:

Si se ha habilitado la seguridad a nivel de datos observados, entonces se filtrará la salida del proceso de auditoría para que los usuarios sólo vean la información de sus bases de datos.

Bajo las opciones de Informe dentro de Añadir la tarea de auditoría hay dos informes de procedimiento, Sucesos pendientes y Transición del estado del suceso. Añada estos dos informes a dos nuevas tareas de auditoría para mostrar los detalles de todos los sucesos de flujo de trabajo y transiciones. Estos dos informes no se filtrarán (no se aplicará el filtro de seguridad a nivel de datos observado). Estos dos informes están disponibles de forma predeterminada en la lista de informes solo para el usuario administrador y los usuarios con el rol de administración.

El botón Columnas adicionales está inhabilitado para las tareas de clasificación.

Clonar una tarea de auditoría: si está clonando un proceso y ha realizado cambios en una tarea clonada antes de guardar el proceso clonado, el flujo de trabajo asociado con la tarea original no se clonará.

La supresión de un estado de suceso solo se permite si el estado no está en el primer estado de cualquiera de los sucesos y si no lo utiliza ninguna acción. La validación proporcionará una lista de sucesos/acciones que impiden que el estado se suprima.

El propietario/creador de un suceso de flujo de trabajo siempre puede ver todos los estados de este suceso, independientemente de qué roles se hayan asignado a estos estados.

Definir una tarea de asesoramiento de seguridad

Si aún no ha empezado a definir un proceso de automatización del flujo de trabajo de cumplimiento, cree un proceso de flujo de trabajo antes de realizar este procedimiento. Si el asesoramiento que se va a utilizar todavía no se ha definido, hágalo primero.

1. Si el panel Añadir tarea nueva no está abierto, pulse Añadir la tarea de auditoría.
2. Pulse el botón Asesoramiento de seguridad.
3. Seleccione un asesoramiento de seguridad en la lista Asesoramiento de seguridad.
4. La selección de Contenido de PDF es Informe (los resultados actuales), Diferencias (diferencias entre un informe anterior y un informe nuevo) e Informes y Diferencias (ambos).
5. Pulse Aplicar.

Nota:

Si se ha habilitado la seguridad a nivel de datos observados, entonces se filtrará la salida del proceso de auditoría para que los usuarios sólo vean la información de sus bases de datos.

Si una tarea de asesoramiento de seguridad está vacía (por ejemplo, un asesoramiento de seguridad con un conjunto de no roles), este asesoramiento de seguridad vacío no se mostrará en la lista desplegable del Creador de auditoría.

Definir una tarea de seguimiento de auditoría de entidad

Si aún no ha empezado a definir un proceso de automatización del flujo de trabajo de cumplimiento, cree un proceso de flujo de trabajo antes de realizar este procedimiento.

1. Si el panel Añadir tarea nueva no está abierto, pulse Añadir la tarea de auditoría.
2. Pulse el botón Seguimiento de auditoría de entidad.
3. Seleccione el tipo de entidad que se va a auditar. En función del tipo seleccionado, se le solicitará que suministre la siguiente información:
    - Objeto: Entre un nombre de objeto.
    - Grupo de objetos: Seleccione un grupo de objetos de la lista.
    - IP de cliente: Especifique una dirección IP de cliente.
    - IP de grupo de clientes: Seleccione un grupo de IP de cliente.
    - IP de servidor: Entre una dirección IP de servidor.
    - Nombre de usuario de aplicación: Especifique un nombre de usuario de la aplicación.
4. Hay varias opciones para las etiquetas de archivo CSV/CEF, Escribir CEF en Syslog, Comprimir y exportar PDF. Consulte Exportar a un archivo CSV o CEF.
5. En el panel Parámetros de tarea, suministre valores de parámetro de tiempo de ejecución (sólo son necesarios los periodos Desde y Hasta).
6. Pulse Aplicar.

Nota: Si se ha habilitado la seguridad a nivel de datos observados, entonces se filtrará la salida del proceso de auditoría para que los usuarios sólo vean la información de sus bases de datos.

Definir una tarea de conjunto de privacidad

Si aún no ha empezado a definir un proceso de automatización del flujo de trabajo de cumplimiento, cree un proceso de flujo de trabajo antes de realizar este procedimiento. Si el conjunto de privacidad que se va a utilizar aún no se ha definido, hágalo primero.

1. Si el panel Añadir tarea nueva no está abierto, pulse Añadir la tarea de auditoría.
2. Pulse el botón Conjunto de privacidad.
3. Seleccione un conjunto de privacidad en la lista Conjunto de privacidad.
4. Seleccione Informar por detalles de acceso o Informar por usuario de aplicación para indicar cómo desea que se muestren y visualicen los resultados.
5. Hay varias opciones para las etiquetas de archivo CSV/CEF, Escribir CEF en Syslog, Comprimir y exportar PDF. Consulte Exportar a un archivo CSV o CEF.
6. Introduzca las fechas de inicio y de finalización para el informe en los cuadros Inicio de periodo y Final de periodo.
7. Pulse Aplicar.

Nota: Si se ha habilitado la seguridad a nivel de datos observados, entonces se filtrará la salida del proceso de auditoría para que los usuarios sólo vean la información de sus bases de datos.

Definir una tarea de proceso de clasificación

Si aún no ha empezado a definir un proceso de automatización del flujo de trabajo de cumplimiento, cree un proceso de flujo de trabajo antes de realizar este procedimiento. Si el proceso de clasificación que se va a utilizar aún no se ha definido, hágalo primero.

1. Si el panel Añadir tarea nueva no está abierto, pulse Añadir la tarea de auditoría.
2. Pulse el botón Proceso de clasificación.
   Nota: Recibirá una alerta de que los procesos de clasificación pueden devolver datos confidenciales y que dichos resultados se añadirán a archivos PDF o CSV.
3. Seleccione un proceso de clasificación en la lista Proceso de clasificación. Pulse Aplicar.

Nota: Si se ha habilitado la seguridad a nivel de datos observados, entonces se filtrará la salida del proceso de auditoría para que los usuarios sólo vean la información de sus bases de datos.

Definir una tarea de canal de información externo

Este tipo de tarea de automatización de flujo de trabajo introduce los datos recopilados por Guardium a una aplicación externa, correlacionando los datos con un formato reconocido por dicha aplicación. Este tipo de tarea es una característica de coste extra, habilitada por un parche.

Nota: Si esta característica se utiliza en un entorno de Gestor central, el parche de canal de información externo debe estar instalado en el Gestor central y en todas las unidades gestionadas en las que se ejecutará la tarea.

Para más información sobre cómo los datos se correlacionan desde Guardium a la aplicación externa, consulte la documentación para la opción que se ha adquirido.

Si aún no ha empezado a definir un proceso de automatización del flujo de trabajo de cumplimiento, cree un proceso de flujo de trabajo antes de realizar este procedimiento.

1. Si el panel Añadir tarea nueva no está abierto, pulse Añadir la tarea de auditoría.
2. Pulse Canal de información externo.

3. Seleccione un tipo de canal de información en la lista Tipo de canal de información.
4. Los controles que aparecen a continuación dependen del tipo de canal de información seleccionado. Consulte Canal de información externo opcional para obtener información adicional sobre tipos de canales de información externos específicos.
5. Seleccione un tipo de suceso en la lista Tipo de suceso.
6. Seleccione un informe desde la Lista de informes. En función del informe seleccionado, se mostrará un número variable de parámetros en el panel Parámetros de tarea.
7. En el recuadro Retardo de extracción, especifique el número de horas durante las que se va a retrasar, o marque el recuadro Continuo para incluir los datos hasta el momento que se ejecuta la tarea de auditoría.
8. En el panel Orígenes de datos, identifique uno o más orígenes de datos para el canal de información externo.
9. Especifique todos los valores de parámetro en el panel Parámetros de tarea. Los parámetros variarán en función del informe seleccionado.
10. Pulse Aplicar.

Ver o firmar resultados

1. Abra los resultados de Automatización de flujo de trabajo de cumplimiento.
2. Si la firma es necesaria, pulse el botón Firmar resultados.
3. Opcional. Para enviar estos resultados a otro usuario, pulse Escalar y vea Reenviar resultados a receptores adicionales (en la sección Escalado).
4. Pulse el enlace Cerrar esta ventana.

Nota: Si hay sucesos pendientes, los resultados no se pueden firmar ni desde el visor de auditoría ni desde la lista de tareas pendientes. Si hay sucesos pendientes y se realiza un intento de firmar los resultados, aparece el mensaje siguiente:

```
No se puede firmar el proceso de auditoría porque tiene sucesos pendientes.

Actualice todos los sucesos pendientes antes de firmar este resultado.
```

Nota: Cuando se examinan los resultados del proceso de auditoría, si un resultado tiene sucesos asociados al mismo, el botón Firmar resultados no está disponible en este resultado hasta que todos los sucesos están en un estado final o este usuario no pueden verlos (debido a la seguridad del nivel de datos).
Nota: Este informe también contiene una fecha u hora de última acción, que se encuentra en una columna entre Receptor y Estado. Este informe muestra que el resultado ha sido firmado por el usuario AAA, pero también cuando este usuario AAA firmó este resultado.

Publicar resultados sin firma ni visualización

1. Abra el panel Lista de tareas pendientes.
2. Pulse el botón Continua para los resultados que desea publicar en el siguiente receptor en la lista de distribución.
3. Pulse el enlace Cerrar esta ventana.

Ver distribución de resultados

1. Abra los resultados de automatización de flujo de trabajo de cumplimiento.
2. Expanda el panel Estado de distribución pulsando el botón (Mostrar detalles).
3. Pulse el enlace Cerrar esta ventana.

Ver comentarios de receptor añadidos a resultados

1. Abra los resultados de automatización de flujo de trabajo de cumplimiento.
2. Expanda el panel Comentarios pulsando el botón Mostrar detalles.
   Nota: Estos son los comentarios que se adjuntaron a los resultados cuando la página de informe se recuperó del sistema Guardium. Si añade comentarios propios, o si otros receptores están añadiendo comentarios simultáneamente, no verá esos comentarios hasta que renueve la página (utilizando la función Renovar del navegador).
3. Pulse el enlace Cerrar esta ventana.

Escalar resultados de proceso

Un receptor de resultados de proceso puede reenviar la notificación de resultados para su revisión y/o aprobación a receptores adicionales. Si escala los resultados a un receptor fuera del seguimiento de aprobación y auditoría original, y los resultados incluyen un archivo CSV, ese archivo no se incluirá con la notificación.

Independientemente de quién sea un receptor de un resultado de auditoría, un escalado puede incluir cualquier usuario del sistema, siempre que esté seleccionado el recuadro Escalar el resultado a todos los usuarios en el menú Configuración > Herramientas y vistas > Perfil global. Una marca de selección en este recuadro escala los resultados del proceso de auditoría a todos los usuarios, incluso si está habilitada la seguridad a nivel de datos en el nivel de datos observado. El valor predeterminado es habilitado. Si el recuadro de selección está inhabilitado (no hay marca de selección en el recuadro de selección), el escalado del proceso de auditoría solo se permitirá a los usuarios en un nivel superior en la jerarquía de usuarios. Si el recuadro de selección está inhabilitado y no hay ninguna jerarquía de usuario, no se permite ningún escalado.

Además, en función de los permisos del suceso, si por ejemplo, el usuario infosec solo puede ver sucesos en status1 y el usuario dba solo puede ver sucesos en status2, el usuario dba recibirá un resultado diferente del resultado que vio el usuario infosec cuando el usuario infosec ha pulsado Escalar. Es posible que infosec escale a dba, y dba reciba un resultado con 0 filas en él.

1. Si los resultados de automatización del flujo de trabajo de cumplimiento que desea reenviar no están abiertos, ábralos ahora.
2. Pulse Escalar.
3. Seleccione el receptor en la lista Receptores.
4. En la columna Acción necesaria, seleccione Revisar (el valor predeterminado) o Revisar y firmar.
5. Pulse el botón Escalado para completar la operación.

Nota:

Los resultados del proceso de auditoría no se pueden escalar a un grupo de usuarios, solo a usuarios o roles.

Cuando se escala a un usuario que ya tiene el resultado en la lista de tareas pendientes del usuario, aparecerá un mensaje emergente solicitándole si se debe enviar un correo electrónico adicional. Si es sí, se enviará al usuario un correo electrónico adicional, pero la lista de tareas pendientes no se incrementará.

Planificar o ejecutar un proceso de automatización de flujo de trabajo de cumplimiento

1. Abra el Creador de procesos de auditoría navegando a Cumplir > Herramientas y vistas > Creador de procesos de auditoría.
2. Seleccione el proceso en la lista de selección de procesos.
3. Pulse Modificar para abrir el panel Definición del proceso de auditoría.
4. Para ejecutar el proceso una vez, pulse Ejecutar una vez ahora, o para definir una planificación para el proceso, pulse Modificar planificación.
   Nota: Una vez que se ha definido una planificación para un proceso, el proceso se ejecuta de acuerdo con esa planificación solo cuando se marca como activo. Para activar o desactivar un proceso de auditoría, consulte la sección siguiente.

Activar o desactivar un proceso de automatización de flujo de trabajo de cumplimiento

Una vez que se ha definido una planificación para un proceso de auditoría, se ejecuta de acuerdo con dicha planificación, solo cuando está marcada como activa.

Para activar o desactivar un proceso de auditoría:

1. Abra el Creador de procesos de auditoría navegando a Cumplir > Herramientas y vistas > Creador de procesos de auditoría.
2. Seleccione el proceso de auditoría en la lista de selección de procesos.
3. Pulse Modificar.
4. En el panel Definición del proceso de auditoría, marque el recuadro Activo para empezar a ejecutar el proceso de acuerdo con la planificación; o deseleccione el recuadro Activo para detener la ejecución del proceso (ignorando cualquier planificación definida).
   Nota: Si está activando el proceso, pero no hay ninguna planificación, pulse Modificar planificación para definir una planificación para ejecutar el proceso.
5. Pulse Guardar.

- Cómo crear un flujo de trabajo de auditoría
  Cree un flujo de trabajo de proceso de auditoría que genere un informe predefinido en una planificación preestablecida, asigne el informe al administrador de base de datos para su revisión y aprobación, y facilite el informe revisado que se está enviando a un supervisor para una revisión y una aprobación adicional.
- Abrir los resultados de proceso de flujo de trabajo
  Utilice Ver para ver los resultados de proceso de flujo de trabajo
- Cómo distribuir el flujo de trabajo a través de grupos de Guardium
  Utilizando la opción de grupo de receptores, defina un único proceso de auditoría de flujo de trabajo de cumplimiento que enviará diferentes resultados a usuarios de Guardium distintos en función de una correlación personalizada predefinida.
- Lista de tareas pendientes de proceso de auditoría
  Este tema describe la Lista de tareas pendientes de proceso de auditoría y los pasos necesarios para abrirla y utilizarla.

Tema principal: Supervisar y auditar

Cómo crear un flujo de trabajo de auditoría

Cree un flujo de trabajo de proceso de auditoría que genere un informe predefinido en una planificación preestablecida, asigne el informe al administrador de base de datos para su revisión y aprobación, y facilite el informe revisado que se está enviando a un supervisor para una revisión y una aprobación adicional.

Acerca de esta tarea

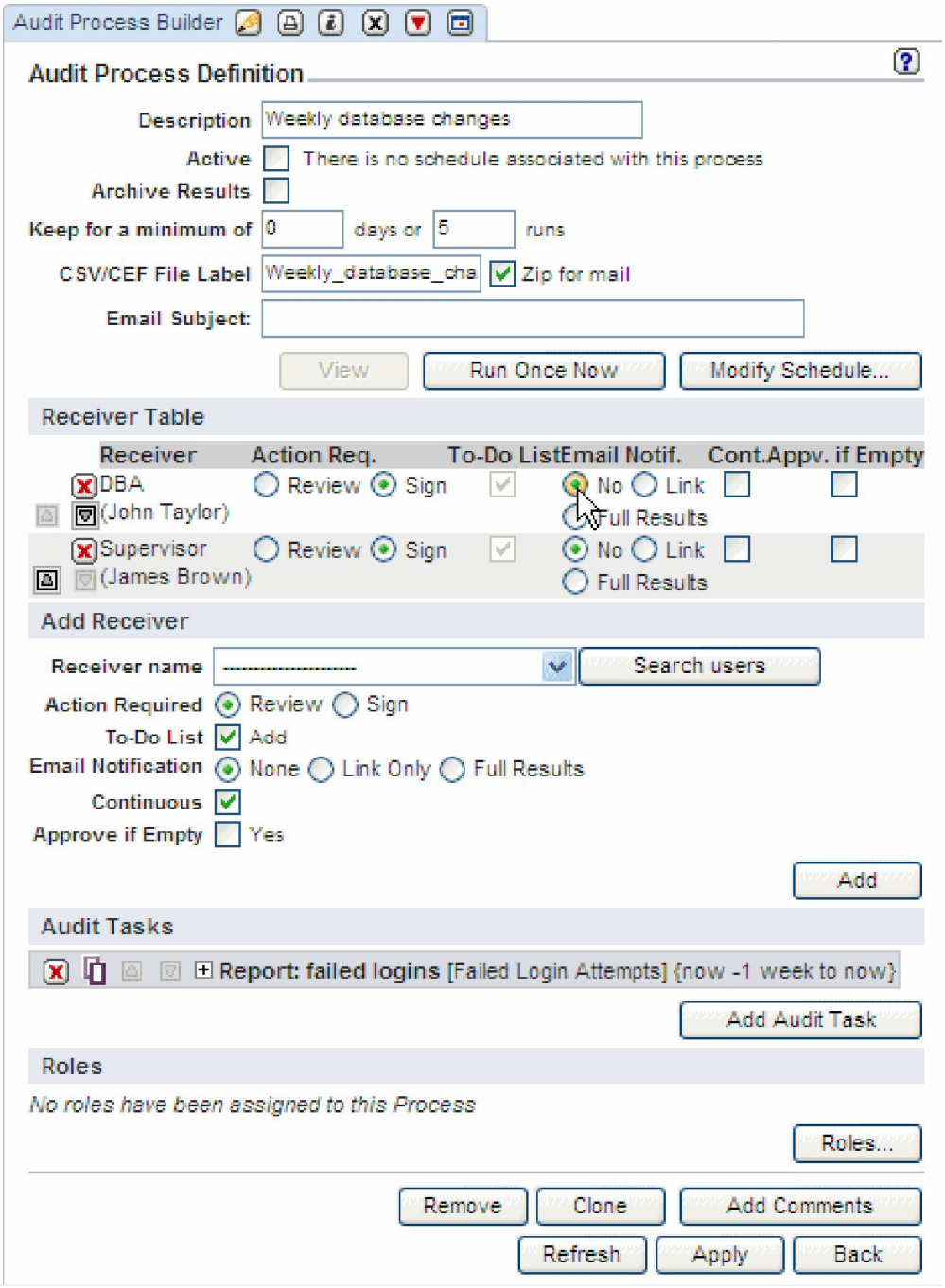
Automatizar los pasos del flujo de trabajo del proceso de auditoría del cliente.

Consulte el tema Automatización de flujo de trabajo de cumplimiento para obtener información adicional acerca de este asunto.

Procedimiento

1. Abra el Buscador de procesos de auditoría navegando a Cumplir > Herramientas y vistas > Creador de procesos de auditoría.
2. Pulse el botón Nuevo para abrir el panel Definición del proceso de auditoría.

   El panel Definición del proceso de auditoría se divide en tres secciones: General, Tabla de receptor y Tareas de auditoría.



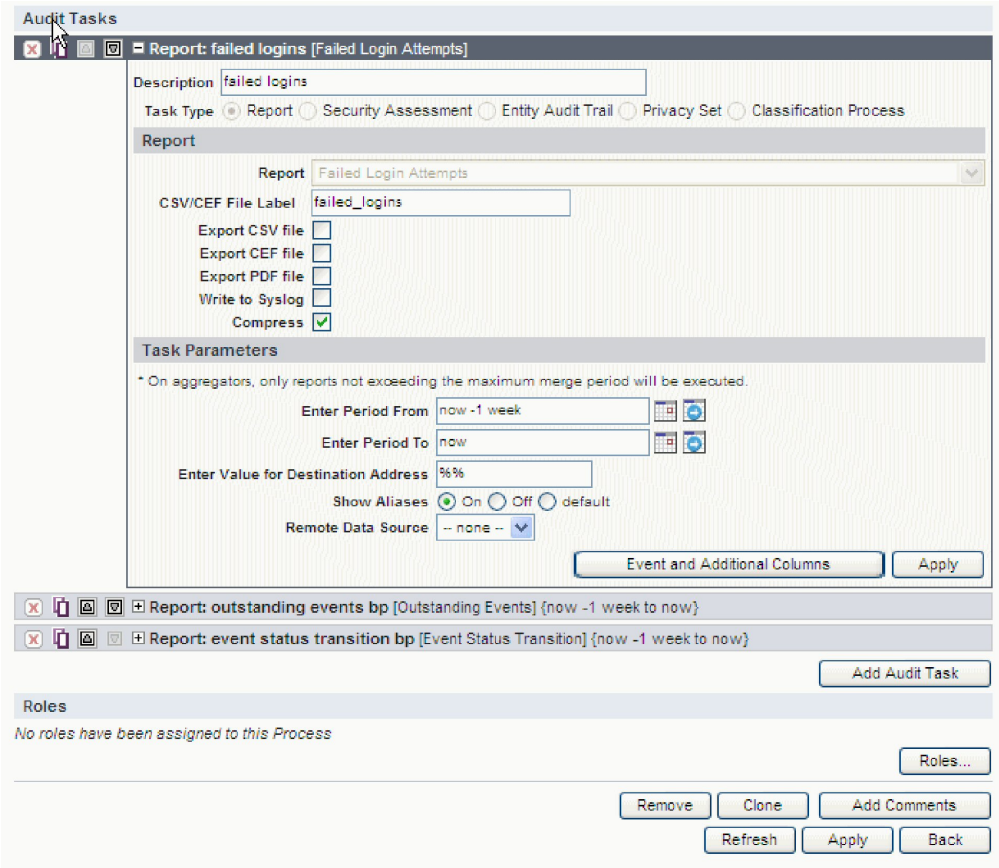
Pantalla de menú del Creador de procesos de auditoría

3. Vaya a la sección General. Especifique un nombre en el recuadro Descripción. No incluya caracteres de apóstrofo.
4. Marque el recuadro Activo para asociar una planificación con el proceso. Se debe definir al menos una tarea de auditoría para poder guardar el proceso.
5. Marque el recuadro Resultados del archivado si desea almacenar los resultados fuera de línea una vez que haya caducado el periodo de retención. Cuando los resultados se han archivado, puede restaurarlos en el dispositivo para volver a visualizarlos más adelante.
6. En los recuadros Mantener durante un mínimo de (n) días o (n) ejecuciones, especifique cuánto tiempo mantener los resultados, ya sea un número de días (0 de forma predeterminada) o un número de ejecuciones (5 de forma predeterminada). Después de esto, los resultados se archivarán (si se marca el recuadro Archivar) y se depurarán del sistema.
7. Si una o más tareas crean archivos CSV o CEF, también puede especificar una etiqueta para que se incluya en todos los nombres de archivo, en el recuadro Etiqueta de archivo CSV/CEF. Estos archivos también se pueden comprimir, o incluirse en un zip, pulsando en el recuadro Comprimir CVS por correo electrónico para añadir una marca de selección.
8. El campo Asunto de correo electrónico en la Definición del proceso de auditoría se utiliza en los correos electrónicos para todos los receptores para ese proceso de auditoría. El sujeto puede contener una (o varias) de las variables siguientes que se sustituirán en el tiempo de ejecución para el asunto:
   - %% ProcessName se sustituirá por la descripción del proceso de auditoría
   - %% ExecutionStart se sustituirá por la fecha y la hora de inicio de la primera tarea.
   - %% ExecutionEnd se sustituirá por la fecha y hora de finalización de la última tarea.

   Después de especificar un asunto, comprobará si hay alguna variable (empezando por%% presente) y garantizará que todas sean variables válidas.
9. Vaya a la sección Receptores. Abra el recuadro desplegable y añada los receptores para el proceso. Consulte Añadir receptores en el tema Automatización de flujo de trabajo de cumplimiento para obtener más información. Son necesarias marcas de verificación para determinar la acción necesaria, adiciones a la lista de tareas pendiente, la notificación a través de notificaciones de correo electrónico y la distribución continua. De nuevo, consulte el apartado Añadir receptores para obtener

información completa sobre cómo establecer estas opciones. En este ejemplo, no marque los recuadros Continuo para los receptores. Si el recuadro de selección Continuo está marcado, la distribución continua al siguiente receptor de la lista sin interrupción. Si el recuadro de selección Continuo no está marcado, la distribución al siguiente receptor se retiene hasta que el receptor actual realiza la acción necesaria (revisar o firmar). En este ejemplo, el DBA necesita ver y firmar el informe antes de que vaya al supervisor.

10. Vaya a la sección Tareas. Debe definir al menos una tarea de auditoría para poder guardar el proceso.
11. Definir una tarea de informe.
    a. Si el panel Añadir tarea nueva no está abierto, pulse Añadir la tarea de auditoría (consulte la ilustración).
    b. Pulse el botón Informe.
    c. Opcionalmente, cree la salida del archivo CSV o CEF y escriba en Syslog.
    d. Especifique todos los valores de parámetro en el panel Parámetros de tarea. Los parámetros variarán en función del informe seleccionado.
    e. Pulse Aplicar.



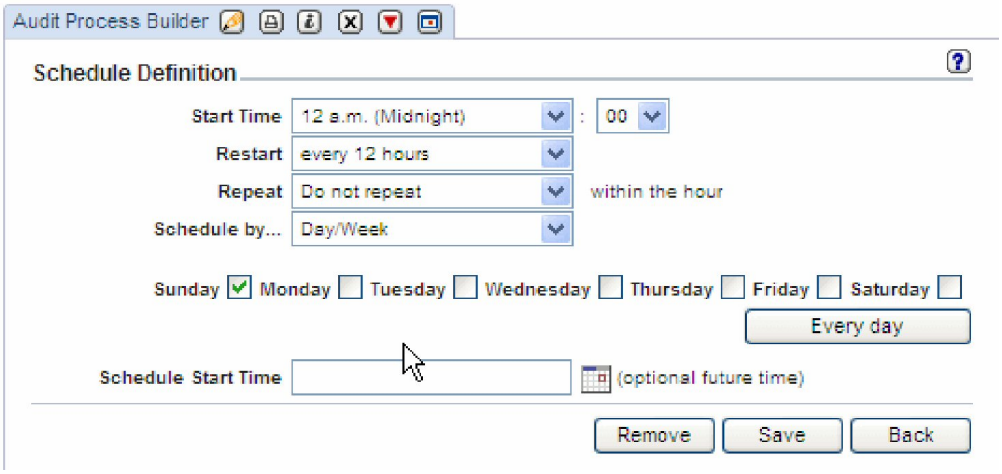
Tarea de auditoría – Informe

12. Opcionalmente, asigne roles de seguridad.
    a. Abra o seleccione el elemento al que desea asignar uno o varios roles de seguridad (por ejemplo, una definición de informe).
    b. Pulse el botón Roles.
    c. En el panel Asignar roles de seguridad, marque todos los roles que desea asignar (solo verá los roles que se han asignado a la cuenta).
    d. Pulse Aplicar.
13. Opcionalmente, añada comentarios
14. Pulse los botones adecuados para planificar o ejecutar un proceso de flujo de trabajo de auditoría (consulte el enlace).
15. Pulse Aplicar.
16. Planificar o ejecutar un proceso de automatización de flujo de trabajo de cumplimiento

Abra el Buscador de procesos de auditoría navegando a Cumplir > Herramientas y vistas > Creador de procesos de auditoría.

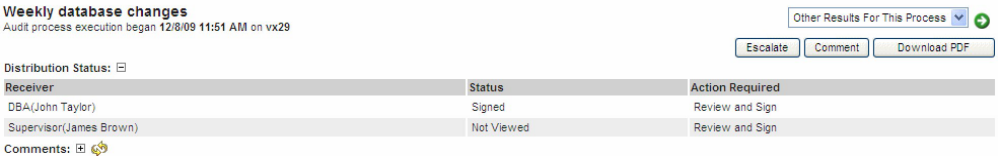
    a. Seleccione el proceso en la lista de selección de procesos.
    b. Pulse Modificar para abrir el panel Definición del proceso de auditoría.
    c. Para ejecutar el proceso una vez, pulse Ejecutar una vez ahora, o para definir una planificación para el proceso, pulse Modificar planificación.

Nota: Una vez que se ha definido una planificación para un proceso, el proceso se ejecuta de acuerdo con esa planificación solo cuando se marca como activo.



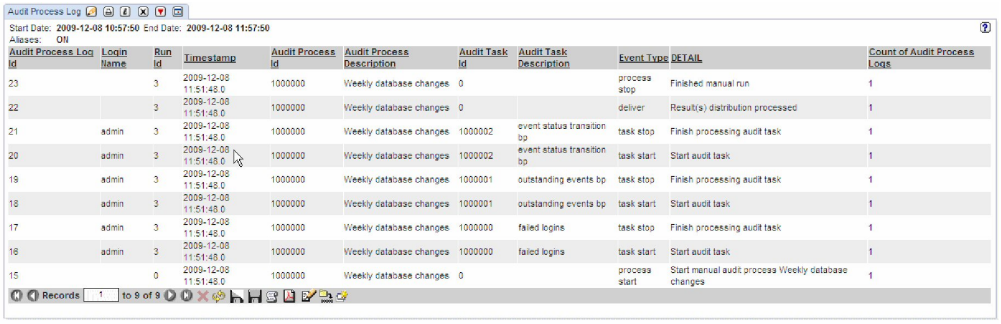
17. Aprobación y revisión del informe

    Después de ejecutar el informe, el estado de distribución puede observarse desde el informe. En el ejemplo, el DBA ha visto y firmado el informe y el supervisor no.



    Estado de distribución

    El informe Registro de proceso de auditoría muestra un registro de actividad detallado para todas las tareas, incluidas las horas de inicio y finalización. Este informe está disponible navegando a Informes > Informes operativos de Guardium > Registro del proceso de auditoría. Las tareas de auditoría muestran las horas de inicio y finalización.



    Ejemplo de Registro del proceso de auditoría

Tema principal: Creación de procesos de auditoría

Abrir los resultados de proceso de flujo de trabajo

Utilice Ver para ver los resultados de proceso de flujo de trabajo

Realice una de las siguientes acciones:

- Abra la lista de tareas pendientes de automatización de flujo de trabajo (consulte Lista de tareas pendientes de proceso de auditoría) y pulse Ver para ver el conjunto de resultados que desea ver o firmar.
- Si ha recibido una notificación por correo electrónico que contiene enlaces de hipertexto a su lista de tareas pendientes o a los resultados, pulse uno de estos enlaces para abrir su lista de tareas pendientes o los resultados directamente desde el correo electrónico. Debe tener acceso al sistema Guardium en la ubicación desde la que está accediendo a su correo electrónico (o estos enlaces no funcionarán). Si no ha iniciado sesión, se le solicitará que inicie sesión en el sistema Guardium.

Nota: Cuando registre una nueva unidad gestionada en un gestor central, es posible que no pueda ver resultados de auditoría. La aplicación no muestra los resultados que tienen una indicación de fecha y hora antes de que la unidad gestionada se registrara en el gestor central. La indicación de fecha y hora del registro utiliza la hora del gestor central, y la indicación de fecha y hora del resultado de la auditoría utiliza la hora del nodo gestionado. Por lo tanto, si la hora del gestor central es anterior a la hora de la unidad gestionada, los resultados generados en la unidad gestionada no son visibles hasta que el tiempo de la unidad gestionada pasa la hora del registro. Esto debe ocurrir en no más de 24 horas, posiblemente menos dependiendo de las ubicaciones de las dos máquinas. Debe poder ver los resultados de los procesos de auditoría en la unidad gestionada dentro de 24 horas de registro.
Tema principal: Creación de procesos de auditoría

Cómo distribuir el flujo de trabajo a través de grupos de Guardium

Utilizando la opción de grupo de receptores, defina un único proceso de auditoría de flujo de trabajo de cumplimiento que enviará diferentes resultados a usuarios de Guardium distintos en función de una correlación personalizada predefinida.

Valor añadido: Configurar un único proceso de auditoría y distribuir los resultados adecuados al gestor correspondiente. Esto ahorra tener que crear procesos de auditoría distintos para receptores diferentes.

Automatización de flujo de trabajo de cumplimiento de IBM Security Guardium's proporciona automáticamente informes, resultados de clasificación y resultados de asesoramiento de seguridad a usuarios de Guardium de forma planificada. Los receptores de resultados pueden definirse como usuarios de Guardium, roles de Guardium o grupos de usuarios.

Por ejemplo, supongamos una gran organización que tenga quince gestores de DBA que necesiten revisar las actividades para los DBA que gestionan sin ver las actividades de los DBA de otros gestores. Una solución sería configurar quince procesos de auditoría separados; uno para cada gestor. Esto tardaría mucho en configurarse y sería difícil de gestionar: cada proceso de auditoría necesita planificarse de forma separada y cualquier cambio global sería necesario realizarse de forma individual para todos los quince procesos de auditoría.

Por otro lado, el método de distribución de grupo de usuarios permite la configuración de un solo proceso de auditoría y distribuye los resultados adecuados a cada gestor basándose en una correlación de gestor/DBA. Este proceso requiere más configuración inicial pero reduce el tiempo de mantenimiento. Solo es necesario planificar un proceso de auditoría y los cambios sólo deben aplicarse en una ubicación.

Correlación de usuarios

El primer paso en el proceso es correlacionar los usuarios con los elementos de datos de Guardium que serán la base para la distribución de informes. El ejemplo que se utilizará en este documento se basará en objetos, pero puede aplicar estos conceptos con cualquier elemento de datos dentro de Guardium.

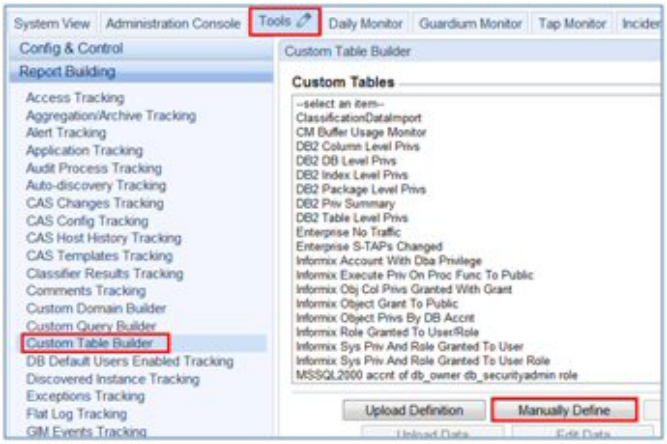
Ejemplo: Tres usuarios tienen la responsabilidad sobre tres conjuntos de tablas distintos, en función de los requisitos de auditoría (PCI, HIPPA y CCI) dentro de un servidor de bases de datos, como se indica a continuación:

Tabla 1. Usuario con tabla/objeto

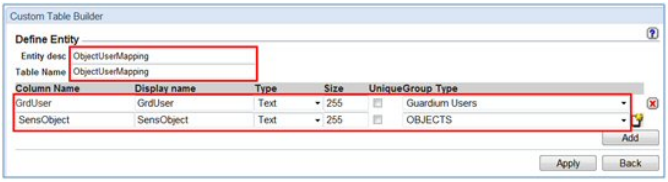
Usuario	Tabla/Objeto
User01	db2inst1.cc_numbers
User01	db2inst1.ccn
User02	db2inst1.ADDRESSES
User02	db2inst1.SSN_NUMBERS
User02	db2inst1.G_CUSTOMERS
User02	db2inst1.G_EMPLOYEES
User02	db2inst1.G_FUNDS
User03	db2inst1.doctor
User03	db2inst1.medicare
User03	db2inst1.med_history

Esta tabla se debe añadir como una tabla personalizada en Guardium, ya sea manualmente o a través de una subida de datos. Los siguientes pasos demuestran cómo crear manualmente una tabla personalizada. Las capturas de pantalla son de la interfaz de usuario "admin", pero también se puede acceder a ellas desde dentro de la interfaz de usuario "user".

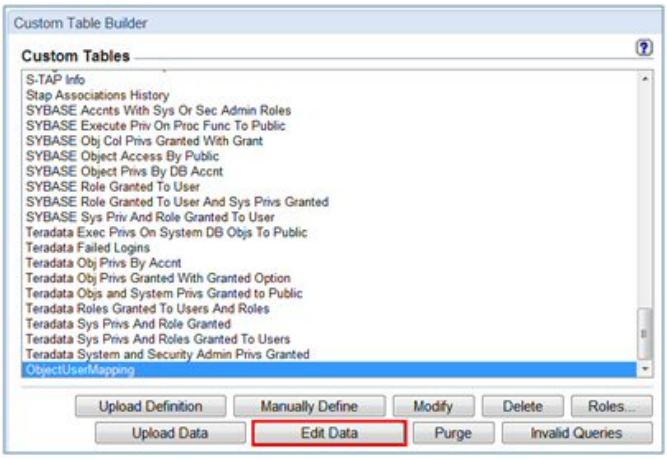
1. Vaya a Informes > Herramientas de configuración de informes > Creador de tablas personalizadasy pulse el botón **Definir manualmente**.



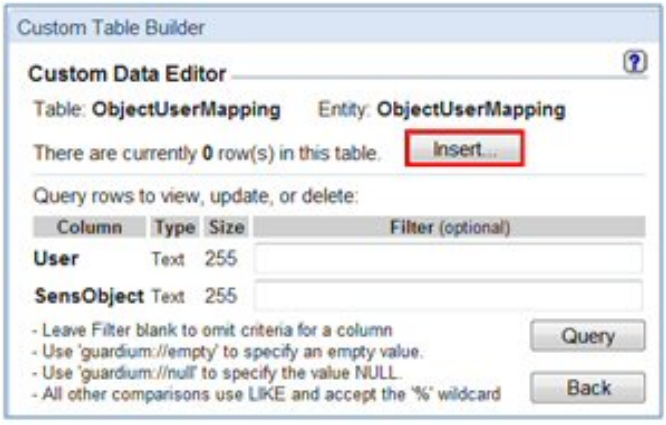
2. En la pantalla **Creador de tablas personalizadas**, defina el diseño de tabla. Asegúrese de que el **Tipo de grupo** coincide con el elemento de datos correcto en Guardium. Pulse **Aplicar** y **Atrás** cuando haya terminado.



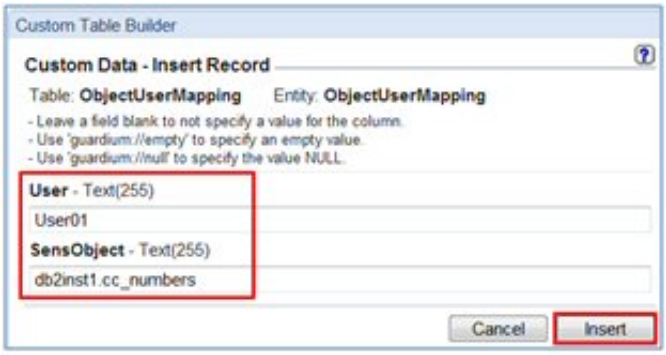
3. Pulse **Editar datos** para añadir manualmente los registros. Tenga en cuenta que, si tiene una gran cantidad de datos, elija **Subir datos** para importar desde un origen de datos externo.



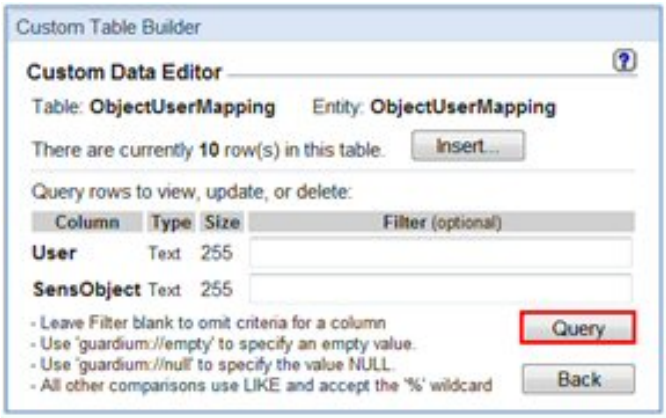
4. Pulse **Insertar**.



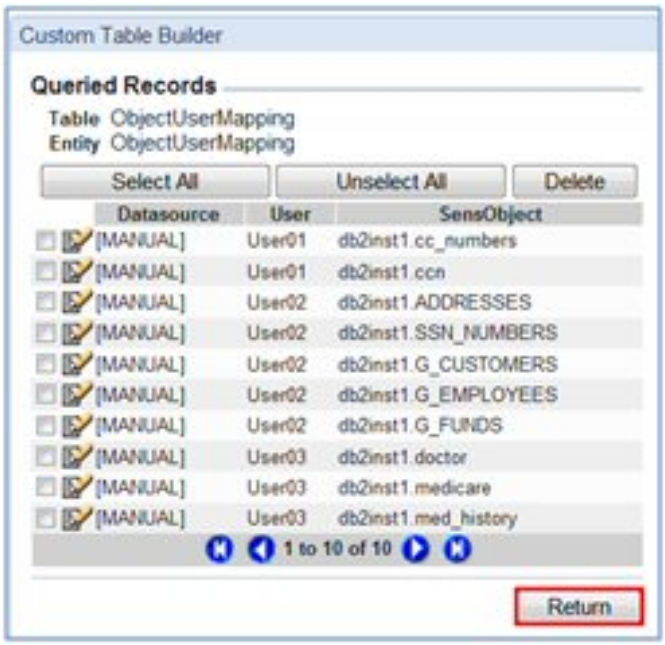
5. Especifique cada combinación de valores y pulse **Insertar** hasta que haya añadido todos los registros necesarios.



6. Cuando haya terminado, pulse el botón **Consultar** para revisar los datos.



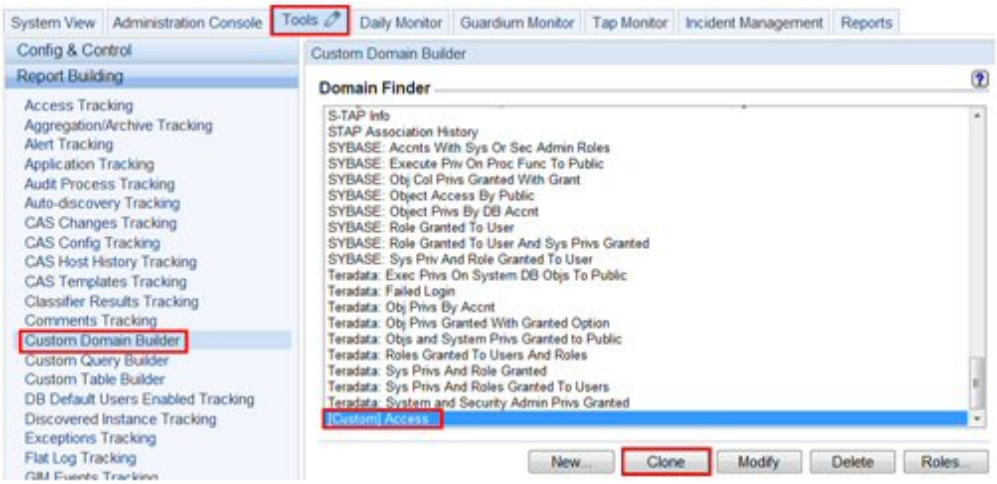
7. Pulse Intro cuando haya terminado.



Dominios personalizados

A continuación, una esta tabla personalizada a la estructura de tabla de Guardium utilizando Dominios personalizados.

1. Vaya a Informes > Herramientas de configuración de informes > Creador de dominios personalizados. Resalte *Acceso [Personalizado]* y pulse **Clonar.**

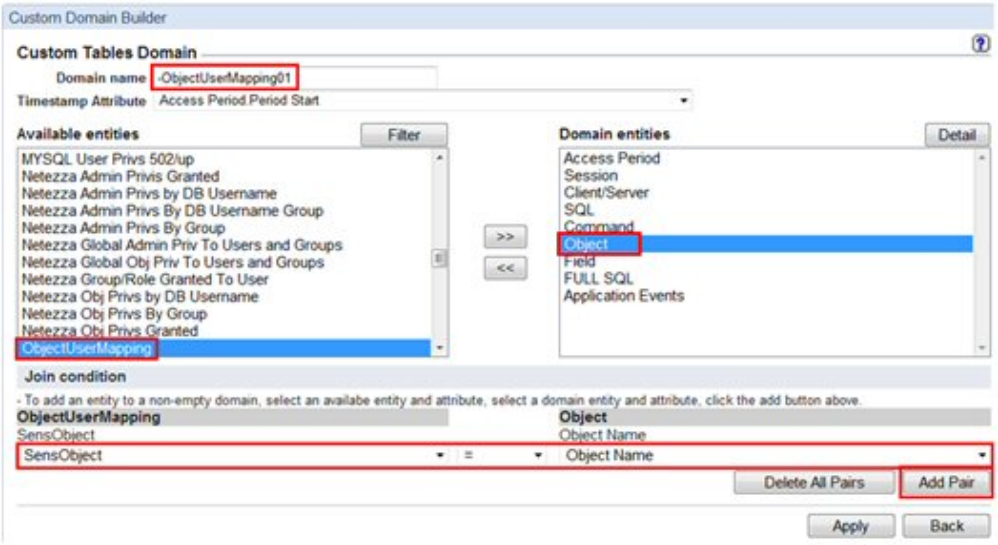


2. En el Creador de dominios personalizados:

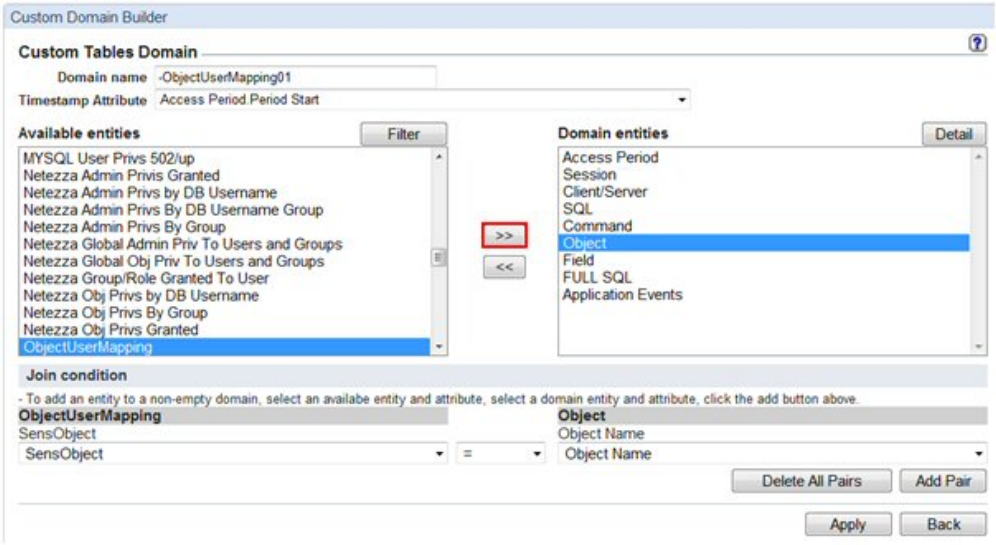
   a. Resalte la nueva tabla creada en **Entidades disponibles.**

   b. Resalte la tabla bajo **Entidades de dominio** a la que le gustaría unir la tabla personalizada.

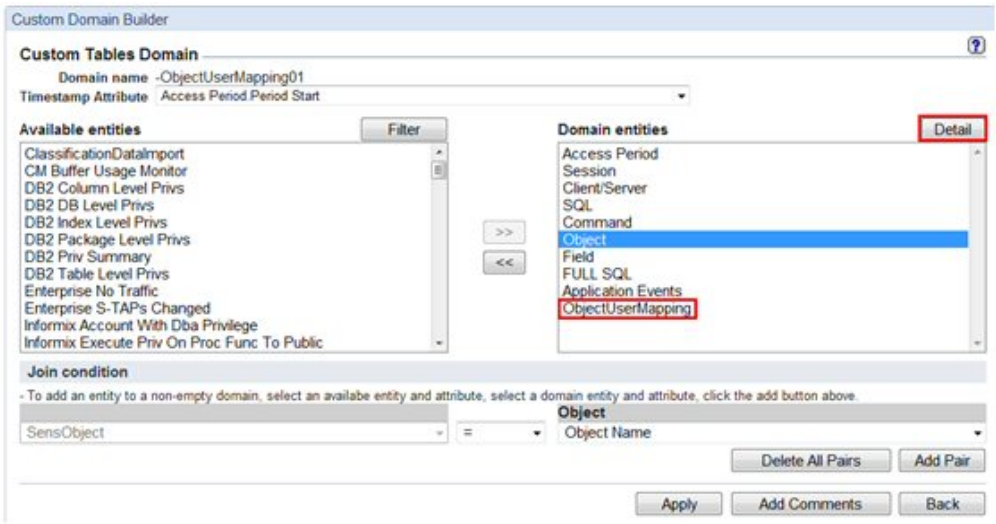
   c. Bajo **Condición de unión**, seleccione los campos de cada tabla en la que desee crear la unión y pulse **Añadir par**.



3. Pulse el botón de las flechas (> >) para mover la tabla personalizada de **Entidades disponibles** a **Entidades de dominio.**

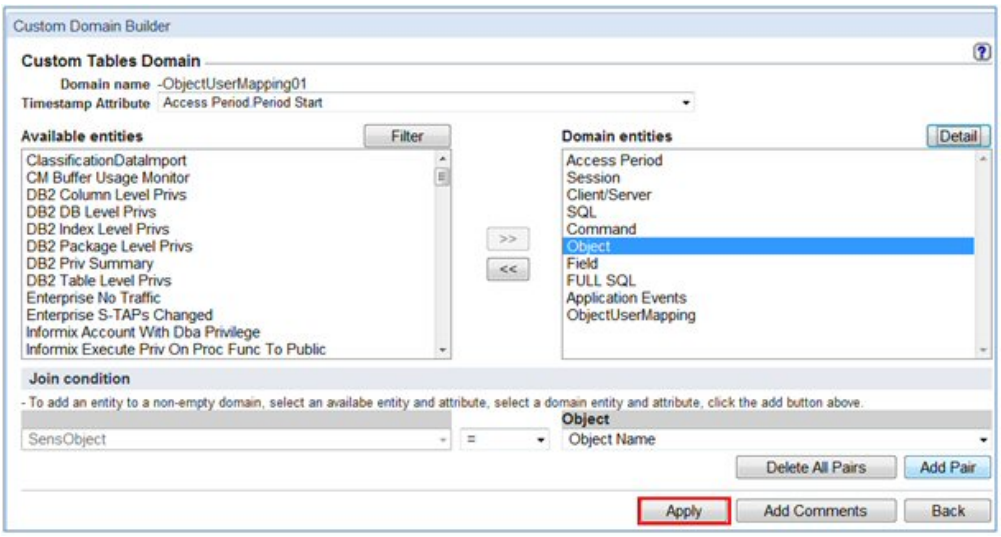


4. Pulse el botón **Detalle** para revisar las uniones.



5. Confirme que las uniones son correctas y pulse **Cerrar**.

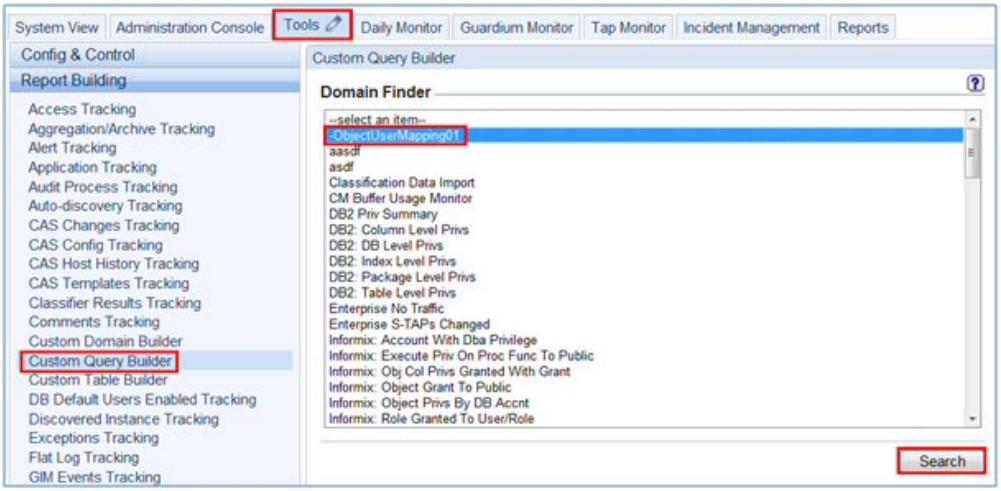
6. Pulse **Aplicar** para guardar el nuevo dominio personalizado.



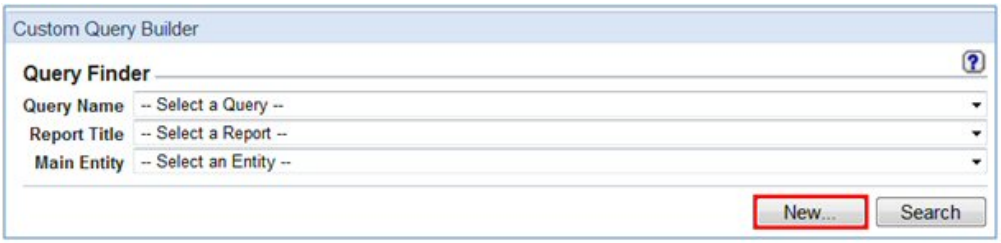
Informe personalizado

A continuación, cree un informe para distribuir a los usuarios.

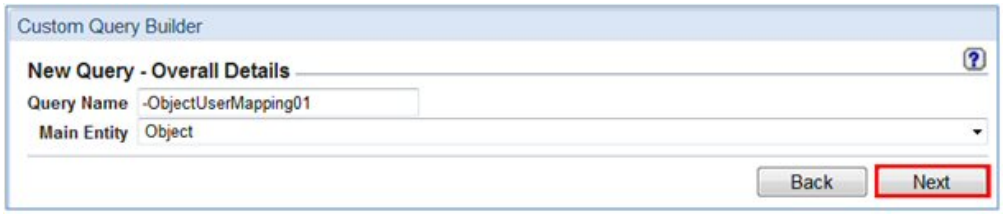
1. Vaya a Informes > Herramientas de configuración de informes > Creador de informes y seleccione el nuevo dominio en el menú desplegable Dominio.



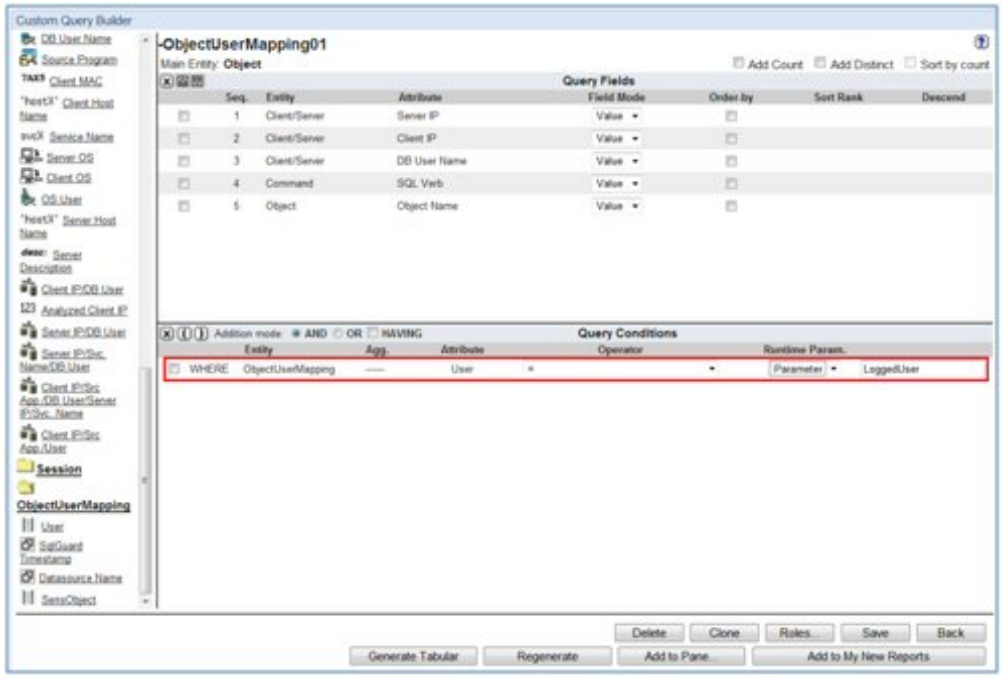
2. Pulse **Nuevo.**



3. Especifique un **Nombre de consulta** y una **Entidad principal** y pulse **Siguiente.**



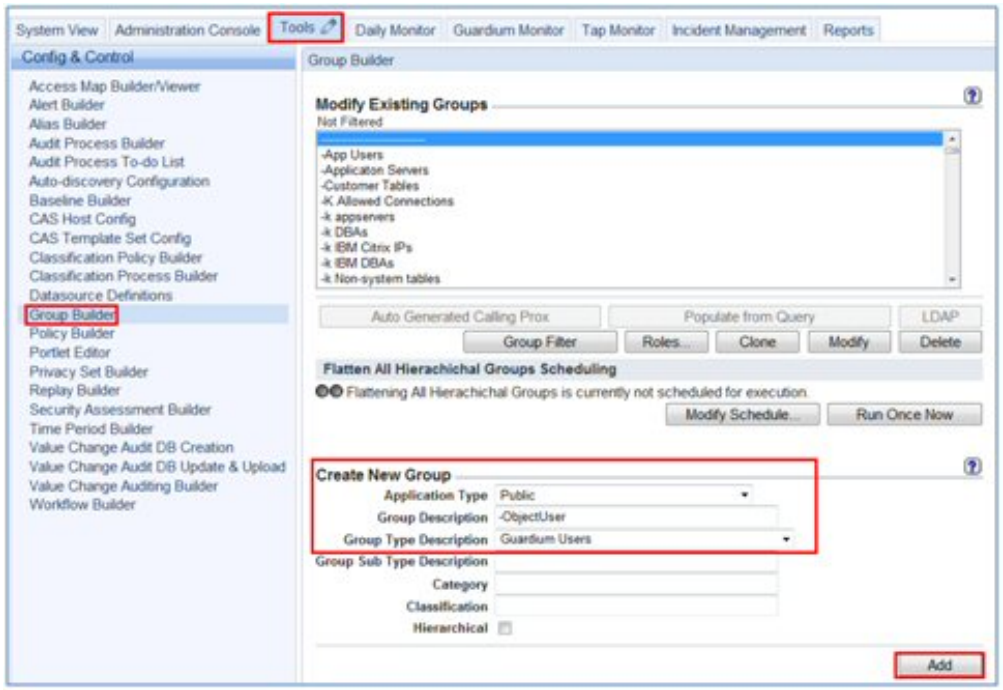
4. Cree un informe nuevo con un parámetro de tiempo de ejecución para el campo de usuario creado en la tabla personalizada.



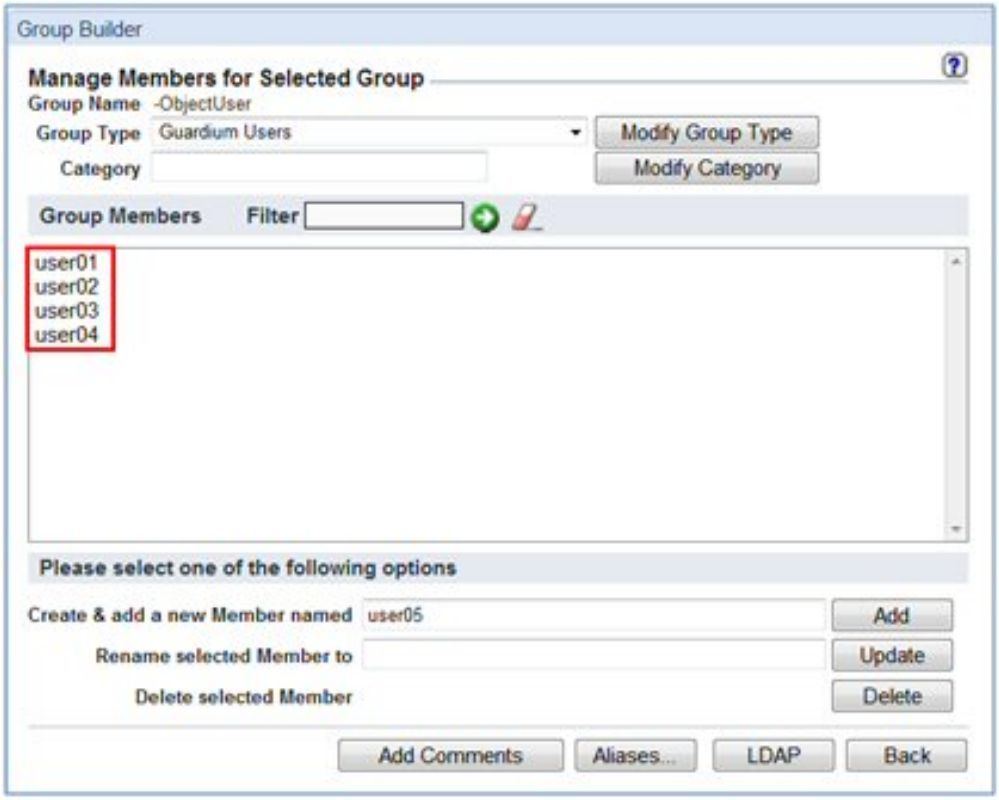
Grupo de usuarios

Cree un nuevo grupo de "Usuarios de Guardium" basado en la tabla personalizada.

1. Vaya a Configuración > Herramientas y vistas > Creador de gruposy cree un nuevo grupo con **Usuarios de Guardium** como el **Tipo de grupo.**

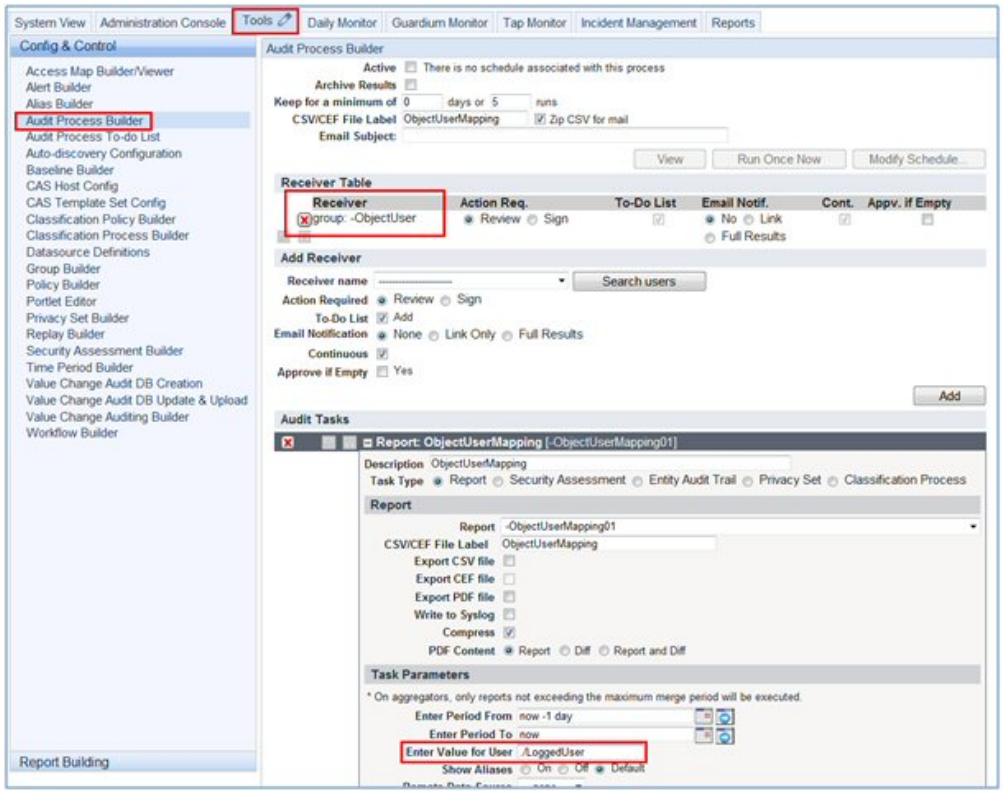


2. Añada todos los usuarios de la tabla personalizada.



Proceso de auditoría

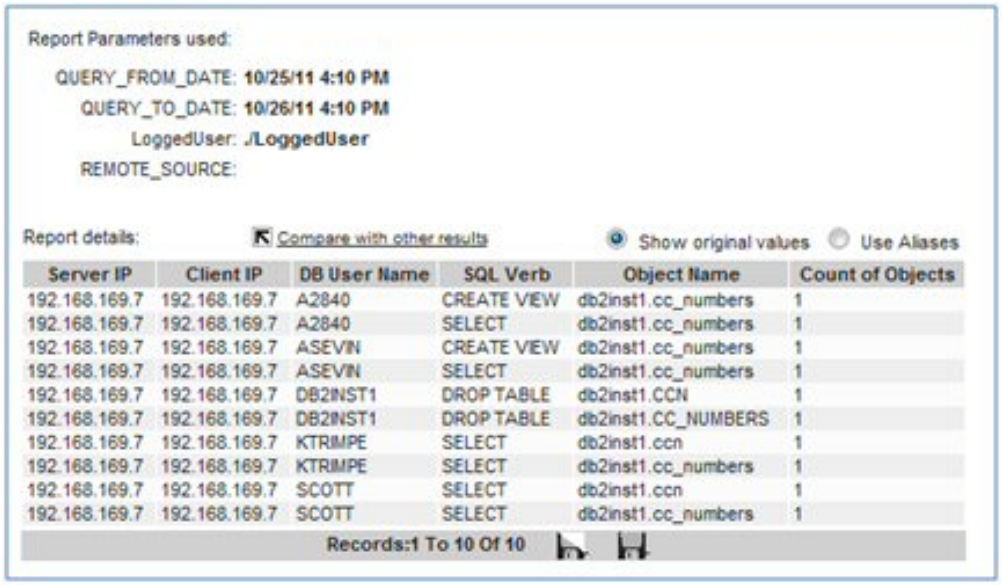
1. Cree un proceso de auditoría.
2. Elija el grupo creado en el grupo de usuarios como el **receptor**
3. Elija el informe personalizado creado en el paso 4 como la tarea.
4. En el parámetro de tiempo de ejecución, especifique el código especial "./LoggedUser". Esto hará que los resultados se distribuyan basándose en la correlación personalizada.
5. Pulse **Ejecutar una vez ahora** para ejecutar el proceso de auditoría.



Cuando se completa el proceso de auditoría, cada receptor debe ser un conjunto de resultados diferente basado en la correlación:

Usuarios

User01



Report Parameters used:

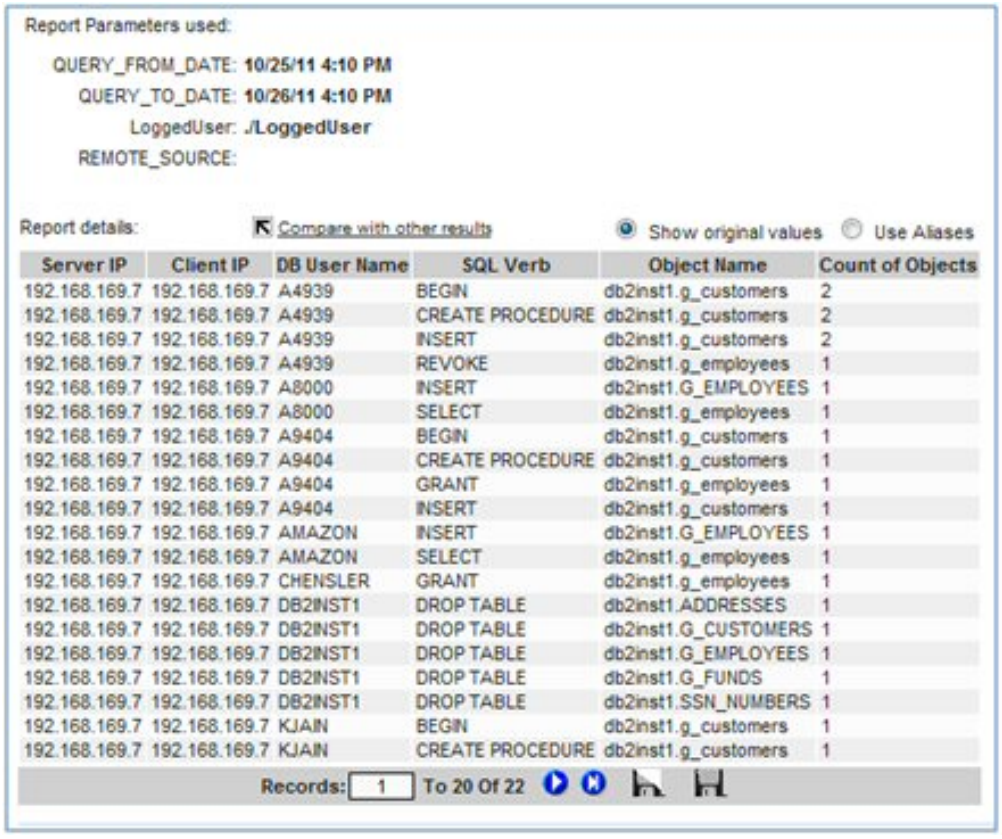
QUERY_FROM_DATE: 10/25/11 4:10 PM
QUERY_TO_DATE: 10/26/11 4:10 PM
LoggedUser: ./LoggedUser
REMOTE_SOURCE:

Report details: Compare with other results — Show original values — Use Aliases

Server IP	Client IP	DB User Name	SQL Verb	Object Name	Count of Objects
192.168.169.7	192.168.169.7	A2840	CREATE VIEW	db2inst1.cc_numbers	1
192.168.169.7	192.168.169.7	A2840	SELECT	db2inst1.cc_numbers	1
192.168.169.7	192.168.169.7	ASEVIN	CREATE VIEW	db2inst1.cc_numbers	1
192.168.169.7	192.168.169.7	ASEVIN	SELECT	db2inst1.cc_numbers	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.CCN	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.CC_NUMBERS	1
192.168.169.7	192.168.169.7	KTRIMPE	SELECT	db2inst1.ccn	1
192.168.169.7	192.168.169.7	KTRIMPE	SELECT	db2inst1.cc_numbers	1
192.168.169.7	192.168.169.7	SCOTT	SELECT	db2inst1.ccn	1
192.168.169.7	192.168.169.7	SCOTT	SELECT	db2inst1.cc_numbers	1

Records:1 To 10 Of 10

User02



Report Parameters used:

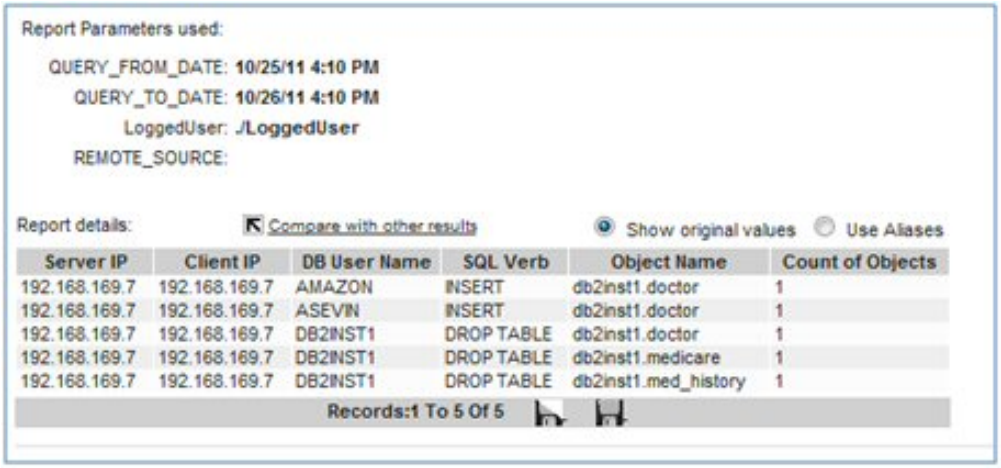
QUERY_FROM_DATE: 10/25/11 4:10 PM
QUERY_TO_DATE: 10/26/11 4:10 PM
LoggedUser: ./LoggedUser
REMOTE_SOURCE:

Report details: Compare with other results — Show original values — Use Aliases

Server IP	Client IP	DB User Name	SQL Verb	Object Name	Count of Objects
192.168.169.7	192.168.169.7	A4939	BEGIN	db2inst1.g_customers	2
192.168.169.7	192.168.169.7	A4939	CREATE PROCEDURE	db2inst1.g_customers	2
192.168.169.7	192.168.169.7	A4939	INSERT	db2inst1.g_customers	2
192.168.169.7	192.168.169.7	A4939	REVOKE	db2inst1.g_employees	1
192.168.169.7	192.168.169.7	A8000	INSERT	db2inst1.G_EMPLOYEES	1
192.168.169.7	192.168.169.7	A8000	SELECT	db2inst1.g_employees	1
192.168.169.7	192.168.169.7	A9404	BEGIN	db2inst1.g_customers	1
192.168.169.7	192.168.169.7	A9404	CREATE PROCEDURE	db2inst1.g_customers	1
192.168.169.7	192.168.169.7	A9404	GRANT	db2inst1.g_employees	1
192.168.169.7	192.168.169.7	A9404	INSERT	db2inst1.g_customers	1
192.168.169.7	192.168.169.7	AMAZON	INSERT	db2inst1.G_EMPLOYEES	1
192.168.169.7	192.168.169.7	AMAZON	SELECT	db2inst1.g_employees	1
192.168.169.7	192.168.169.7	CHENSLER	GRANT	db2inst1.g_employees	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.ADDRESSES	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.G_CUSTOMERS	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.G_EMPLOYEES	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.G_FUNDS	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.SSN_NUMBERS	1
192.168.169.7	192.168.169.7	KJAIN	BEGIN	db2inst1.g_customers	1
192.168.169.7	192.168.169.7	KJAIN	CREATE PROCEDURE	db2inst1.g_customers	1

Records: 1 To 20 Of 22

User03



Report Parameters used:

QUERY_FROM_DATE: 10/25/11 4:10 PM
QUERY_TO_DATE: 10/26/11 4:10 PM
LoggedUser: ./LoggedUser
REMOTE_SOURCE:

Report details: Compare with other results Show original values Use Aliases

Server IP	Client IP	DB User Name	SQL Verb	Object Name	Count of Objects
192.168.169.7	192.168.169.7	AMAZON	INSERT	db2inst1.doctor	1
192.168.169.7	192.168.169.7	ASEVIN	INSERT	db2inst1.doctor	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.doctor	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.medicare	1
192.168.169.7	192.168.169.7	DB2INST1	DROP TABLE	db2inst1.med_history	1

Records:1 To 5 Of 5

Tema principal: Creación de procesos de auditoría

Lista de tareas pendientes de proceso de auditoría

Este tema describe la Lista de tareas pendientes de proceso de auditoría y los pasos necesarios para abrirla y utilizarla.

Hay varias formas de abrir la Lista de tareas pendientes de proceso de auditoría que incluyen:

- Pulse el icono en el banner de página.
- Vaya a Cumplir > Herramientas y vistas > Lista de tareas pendientes de proceso de auditoría.
- Si ha recibido una notificación por correo electrónico, pulse el enlace Lista de tareas pendientes para abrir la lista de tareas pendientes. De forma alternativa, pulse el enlace de informe para abrir los resultados. En ambos casos, debe estar accediendo a su correo desde una ubicación desde donde se pueda acceder al sistema Guardium.

Los siguientes pasos describen cómo utilizar la Lista de tareas pendientes de proceso de auditoría:

1. Seleccione el usuario cuya Lista de tareas pendientes desea abrir, ya sea abriendo el menú desplegable o pulsando Buscar usuarios. Se le informará si la lista está vacía.
2. Como administrador, puede realizar cualquier acción en cualquier entrada de la lista de tareas pendientes. Todas las acciones que realice se anotan, lo que indica que el administrador ha realizado la acción en nombre del usuario.
3. Las opciones disponibles para la entrada de la lista de tareas pendientes son Ver, Bajar como PDF y Firmar resultados visualizados.

   La selección de Contenido de PDF es: Informe (los resultados actuales), Diferencias (diferencias entre un informe anterior y un informe nuevo) e Informes y Diferencias (ambos).

   Nota: La selección de Contenido de PDF se aplica tanto a archivos adjuntos PDF como a archivos de exportación PDF. El resultado Diferencias solo se aplica después de la primera vez de ejecutar esta tarea. No hay Diferencias con un resultado anterior si no hay ningún resultado anterior. El número máximo de filas que se pueden comparar a la vez es de 5000. Si el número de filas de resultados supera el máximo, el mensaje `primero comparar solo 5000 filas` aparecerá en el resultado de diferencias.
4. Pulse el icono de flechas en círculo para Renovar el conjunto.

Nota: Para enviar archivos a un servidor externo sin enviar un correo electrónico y sin añadir resultados a la lista de tareas pendientes, defina un proceso de auditoría sin receptores. Asimismo, desmarque el recuadro de selección de lista de tareas pendientes en la sección Añadir receptor y elimine/no añada ningún receptor en la sección del receptor para no añadir resultados a la lista de tareas pendientes.

Listas de tareas pendientes y seguridad a nivel de datos

La Lista de tareas pendientes tiene un menú desplegable para ver las listas de tareas pendientes de otros usuarios. A diferencia del menú desplegable de usuarios con el rol admin, el menú desplegable para el resto de los usuarios incluirá SOLO usuarios bajo el usuario actual en la jerarquía de seguridad a nivel de datos (DLS). Si el usuario tiene el rol exento, todos los usuarios se muestran en el menú desplegable. Los usuarios con el rol admin pueden ver todos los usuarios en el menú desplegable.

Cuando un usuario accede a los resultados de otro usuario, los datos presentados en el informe se filtran de acuerdo con la seguridad a nivel de datos y el rol del usuario seleccionado (por ejemplo, en el caso de un flujo de trabajo personalizado, los datos se filtran según el rol del usuario seleccionado y el estado definido para dicho rol).

Si un usuario con rol admin accede a un resultado de un usuario que está bajo la jerarquía, entonces se comporta como se explica en el párrafo anterior. Si el administrador accede a un resultado de un usuario que no está debajo en la jerarquía, entonces mostrará el resultado utilizando la seguridad a nivel de datos del administrador y se mostrará para todos los roles.

Cuando se añade un resultado a la lista de tareas pendientes de un usuario debido a un cambio en un estado de un suceso, si el resultado no se encontraba anteriormente en la lista de tareas pendientes, se envía un correo electrónico al usuario. El correo electrónico no contendrá un PDF, sólo una notificación y un enlace.

Si un usuario va a alguna lista de tareas pendientes de otro usuario, un mensaje indicará qué usuario está determinando el filtrado de DLS.

Tema principal: Creación de procesos de auditoría

Auditoría e informes

Guardium organiza los datos que recopila en un conjunto de dominios. Cada dominio contiene un tipo diferente de información relativa a un área específica de interés: acceso a datos, excepciones, infracciones de política, etc.

Todos los dominios y su contenido se describen en el apéndice Dominios, entidades y atributos.

Hay un creador de consultas separado para cada dominio y el acceso al mismo se controla mediante roles de seguridad. Independientemente del dominio, se utiliza la misma herramienta de creación de propósito general para crear todas las consultas. Para obtener instrucciones detalladas acerca de cómo crear consultas, consulte Consultas.

Además de un conjunto estándar de dominios, los usuarios pueden definir dominios personalizados para que contengan información que se puede subir al dispositivo de Guardium. Por ejemplo, una empresa puede tener una tabla que relacione nombres de usuario de base de datos genéricos (hr23455 o qa4872, por ejemplo) con personas reales (Paula Smith, John Doe). Una vez que se sube la tabla, los nombres reales se pueden visualizar en los informes de Guardium desde el dominio personalizado. Para obtener información más detallada sobre cómo definir y utilizar dominios personalizados, consulte la Correlación de datos externos.

Tema principal: Supervisar y auditar

Correlación de datos externos

Este tema describe la creación de tablas personalizadas para la información de empresa que se necesita además de los datos internos de Guardium existentes.

Muchos clientes tienen información valiosa en muchas bases de datos diferentes de su entorno. Resulta extremadamente útil para un informe de auditoría, para correlacionar la información relevante para que estos informes sean útiles y fáciles de entender. La correlación de datos externos le permite crear tablas personalizadas en el dispositivo de Guardium para la información de empresa necesaria además de los datos internos de Guardium existentes. Puede hacerlo de forma manual dentro de la GUI o basándose en una tabla existente en un servidor de bases de datos. A continuación, se pueden crear consultas e informes para esta información como si fueran datos predefinidos.

Existe una distinción entre una tabla personalizada, un dominio personalizado y una consulta personalizada.

Por ejemplo, tal vez exista una tabla en un servidor de bases de datos que contenga todos los empleados, sus nombres de usuario de base de datos y el departamento al que pertenecen (por ejemplo, desarrollo, financiero, marketing, RRHH, etc.) . Si sube esta tabla y todos sus datos, puede realizar una referencia cruzada de esta tabla con las tablas internas de Guardium para ver, por ejemplo, qué empleados del departamento de marketing están accediendo a la base de datos financiera (que puede constituir una actividad sospechosa).

Para acceder a la ayuda de la Despensa de datos, pulse Despensa de datos.

Tablas personalizadas

Una tabla personalizada contiene uno o más atributos que el usuario desea tener disponibles en el dispositivo Guardium. Por ejemplo, es posible que tenga una tabla de base de datos existente que relacione nombres de usuario codificados con nombres reales. En el tráfico de red, solo se verán los nombres codificados. Al definir una tabla personalizada en el dispositivo Guardium y al subir datos para dicha tabla desde la tabla existente, podrá relacionar los nombres reales y los codificados.

Antes de definir una tabla personalizada, primero verifique que los datos que necesita de la base de datos existente son un tipo de datos soportado. Un tipo de datos está soportado si se toma como uno de los siguientes tipos SQL por el controlador JDBC subyacente: INTEGER, BIGINT, TINYINT, BIT, DECIMAL, DOUBLE, FLOAT, NUMERIC, REAL, CHAR, VARCHAR, DATE, TIME, TIMESTAMP. La siguiente tabla resumen algunos de los tipos de datos soportados y no soportados para subir a una tabla personalizada.

Tipos de datos soportados y no soportados para tablas personalizadas

Utilice esta tabla para ver que los tipos de datos soportados y no soportados existen para determinadas bases de datos.

Tabla 1. Tipos de datos soportados y no soportados para tablas personalizadas

Bases de datos	Tipos de datos soportados	Tipos de datos no soportados
Oracle	float number char varchar2 date nchar nvarchar2	long clob raw nclob longraw bfile rowid urowid blob
DB2	char varchar bigint integer smallint real double decimal date time timestamp	blob clob longvarchar datalink
Sybase	char nchar varchar nvarchar int smallint tinyint datetime smalldatetime	text binary varbinary image timestamp
MS SQL	bigint bit char datetime decimal float int money nchar numeric nvarchar real smalldatetime smallint tinyint smallmoney varchar unique identifier	text
Informix	char nchar integer smallint decimal smallfloat float serial date money varchar nvarchar datetime	text
MY SQL	bigint decimal int mediumint smallint tinyint double float date datetime timestamp time year char binary enum set	longtext tinyblob tinytext blob text mediumblob mediumtext longblob longtext

Nota: Se puede capturar el valor de blob (incluso un valor de 1K) en SQL dinámico, pero no se puede capturar el valor de blob del mismo tamaño en SQL estático.

Archivar y restaurar tabla personalizada

La pantalla Creador de tablas personalizadas tiene un botón denominado Depurar/Archivar.

La pantalla Depurar datos de tabla personalizada tiene un recuadro de selección para Archivar. La selección de este recuadro da como resultado que los datos de la tabla personalizada se incluyan en el archivado de datos normal.

Estos datos de tabla personalizada se archivan de acuerdo con la fecha de la columna SQLGUARD_TIMESTAMP de la tabla personalizada.

Los datos de la tabla personalizada se pueden archivar desde un recopilador o un agregador.

Los datos de la tabla personalizada archivada desde un recopilador se pueden restaurar en cualquier recopilador o agregador gestionado por el mismo Gestor central como el recopilador de origen (los metadatos deben estar presentes).

Los datos de la tabla personalizada archivada desde un agregador pueden restaurarse en cualquier agregador gestionado por el mismo Gestor central que el agente de origen.

Si el archivo que se va a restaurar en un sistema Guardium no tiene los metadatos, los datos de la tabla personalizada no se restauran.

Si la estructura de la tabla personalizada ha cambiado entre el momento del archivado y el momento de la restauración de una forma que da como resultado un error de SQL (por ejemplo, columnas eliminadas o tipo cambiado), aparecerá un mensaje de aviso en el informe de actividad de agregación/archivado y los datos no se restaurarán.

Si una tabla personalizada se establece para que se depure mediante la depuración predeterminada, los datos restaurados se conservarán durante el número de días especificado en la pantalla de restauración.

Si la tabla personalizada se establece de modo que sobrescriba los datos cuando se suba, los datos restaurados se suprimirán en el momento en que se realice una subida.

Dominios personalizados

Un dominio personalizado contiene una o más tablas personalizadas. Si contiene varias tablas, debe definir las relaciones entre las tablas al definir el dominio personalizado.

Consultas personalizadas

Una consulta personalizada accede a los datos desde un dominio personalizado. El Creador de consultas personalizadas se utiliza para crear consultas en dominios personalizados. A continuación, se pueden utilizar consultas personalizadas como cualquier otra consulta para generar informes o tareas de auditoría, rellenar grupos o definir alias.

Informes de titularidad de base de datos

Los Informes de titularidad de BD utilizan la característica Dominio personalizado para crear enlaces entre los datos externos de la base de datos seleccionada con los datos internos de los informes de titularidad predefinidos. Consulte el tema, Enlazar datos externos con datos internos, sobre este asunto. Consulte el apartado Informes de titularidad de base de datos para obtener más información sobre cómo utilizar los informes de titularidad de base de datos predefinidos. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador Titularidades de BD.

Crear una tabla personalizada

Abra el Creador de tablas personalizadas navegando a uno de lo siguiente:

- Cumplir > Creación de informes personalizados > Creador de tablas personalizadas
- Informes > Herramientas de configuración de informes > Creador de tablas personalizadas

Subir una definición de tabla

La creación de una tabla personalizada se puede llevar a cabo subiendo una definición de tabla y accediendo a sus metadatos desde el servidor de bases de datos en el que están definidos los metadatos.

Nota: Las tablas personalizadas subidas a Guardium son componentes opcionales habilitados por la clave de producto. Si estos componentes no se han habilitado, las opciones de Tablas personalizadas listadas no aparecerán en la selección Creador de tablas personalizadas.

1. Abra el Creador de tablas personalizadas.
2. Pulse Subir definición para abrir el panel Importar estructura de datos. No es necesario para seleccionar un elemento
3. Especifique una descripción para la tabla en el campo Descripción entidad. Se trata del nombre que utilizará para hacer referencia a la tabla cuando se crea una consulta personalizada.
4. Escriba el nombre de tabla de base de datos para la tabla en el campo Nombre de tabla. Es el nombre que utilizará para crear la tabla en la base de datos local.
5. Especifique una sentencia SQL válida para la tabla en el campo Sentencia SQL. El conjunto de resultados devuelto por la sentencia SQL debe tener la misma estructura que la tabla personalizada definida. Por ejemplo, si la tabla personalizada contiene todas las columnas de la tabla denominada my_table, escriba select * from my_table.
   Nota:

   No incluya ningún carácter de nueva línea en la sentencia SQL. Todas las columnas deben denominarse de forma explícita; utilice un alias de columna si es necesario.

6. Pulse Añadir origen de datos para abrir el Buscador de orígenes de datos en una ventana distinta. Esto permitirá definir dónde se encuentra la base de datos externa y las credenciales necesarias para recuperar la definición de tabla y el contenido de la tabla más adelante en el proceso.
7. Utilice el Buscador de orígenes de datos para identificar la base de datos desde la que se subirá la definición de tabla.
8. Pulse Recuperar para subir la definición de tabla. Esto ejecutará la sentencia SQL y recuperará la estructura de tabla. La solicitud SQL se envía a la base de datos externa desde el sistema Guardium. Recuerde que solo se está subiendo la definición y que puede subir los datos más adelante.

Definir manualmente una definición de tabla

1. Abra el Creador de tablas personalizadas.
2. Pulse Definir de forma manual para abrir el panel Definir entidad.
3. Especifique una descripción para la tabla en el campo Descripción entidad. Se trata del nombre que utilizará para hacer referencia a la tabla cuando se crea una consulta personalizada. No se permite utilizar caracteres especiales `\ $| &; ' ` "` en la descripción de entidad.
4. Escriba el nombre de tabla de base de datos para la tabla en el campo Nombre de tabla. Es el nombre que utilizará para crear la tabla en la base de datos local.
5. Para cada columna de la tabla que se va a definir:
   - Especifique un nombre en el recuadro Nombre de columna. Este será el nombre de la columna en la tabla de base de datos.
   - Especifique un nombre en el recuadro Nombre de visualización. Es el nombre que utilizará para hacer referencia al atributo en el Creador de dominios y el Creador de consultas personalizadas.
   - Seleccione un tipo de datos (Texto, Fecha, Entero, Flotante o Indicación de fecha y hora).
   - Para un atributo de texto, especifique el número máximo de caracteres en el recuadro Tamaño. (El recuadro Tamaño no está disponible para otros tipos de datos).
   - Si se va a aplicar la exclusividad en la columna, seleccione el recuadro Exclusivo.
   - Si el atributo que se está definiendo corresponde a un tipo de grupo, seleccione ese tipo de grupo en la lista Tipo de grupo.
   - Pulse Añadir para añadir la columna.
6. Utilice la lista desplegable Clave de entidad para identificar qué columna se utilizará como clave de entidad. La clave de entidad se utiliza en el creador de consultas al seleccionar el recuento.

7. Si se realizan cambios adicionales después del botón Añadir como, por ejemplo, la supresión de una columna, o el cambio de un atributo, pulse Aplicar para guardar los cambios.
8. Pulse Hecho cuando haya añadido todas las columnas para la tabla.

Modificar una definición de tabla

Si modifica la definición de una tabla personalizada, puede invalidar informes existentes basados en consultas utilizando dicha tabla. Por ejemplo, una consulta existente puede hacer referencia a un atributo que se ha suprimido, o cuyo tipo de datos se ha cambiado. Al aplicar cambios en una tabla personalizada, si se ha creado alguna consulta utilizando atributos de dicha tabla, las consultas se visualizan en el panel Lista de consultas. Nota: También puede utilizar Modificar para ver y validar las estructuras de tabla que se han importado.

1. Abra el Creador de tablas personalizadas.
2. Elija una tabla personalizada pulsando en la etiqueta de entidad y resáltela.
3. Pulse Modificar para abrir el panel Modificar entidad.
4. Consulte Definición de una tabla manualmente para obtener ayuda.
5. Cuando se aplican cambios en una tabla personalizada, si se pueden invalidar algunas de las consultas debido a la modificación del atributo de dicha tabla, las consultas se visualizan en el panel Lista de consultas. Utilice el panel Lista de consultas para elegir y cambiar consultas. No tiene que realizar todos los cambios inmediatamente ya que siempre puede retroceder y utilizar la opción Consultas no válidas.

Consultas no válidas

Si modifica la definición de una tabla personalizada, puede invalidar informes existentes basados en consultas utilizando dicha tabla. Por ejemplo, una consulta existente puede hacer referencia a un atributo que se ha suprimido, o cuyo tipo de datos se ha cambiado. Es conveniente comprobar si hay consultas no válidas después del proceso de modificación de tabla.

1. Abra el Creador de tablas personalizadas.
2. Pulse Consultas no válidas.
3. Las consultas se visualizan en el panel Lista de consultas. Utilice el panel Lista de consultas para elegir y cambiar consultas.

Depurar datos de la tabla personalizada

Se pueden depurar datos de tablas personalizadas en el servidor de Guardium a petición, o de forma planificada.

1. Abra el Creador de tablas personalizadas.
2. Elija una tabla personalizada pulsando en el nombre de tabla y resaltándola.
3. Pulse Depurar para abrir el panel Depurar datos de tabla personalizada.
4. Pulse Depurar todo para depurar ahora.
   Nota: La depuración Ejecutar una vez ahora buscará la retención en la tabla RESTORED_DATA. Depurar todo depurará todos los registros suprimidos sin comprobar la retención.
5. En el panel Configuración, especifique la antigüedad de los datos que se van a depurar, como un número de días, semanas o meses anteriores a la fecha de la operación de depuración.
6. Pulse Ejecutar una vez ahora para ejecutar una vez una operación de depuración de planificación.
7. Pulse Modificar planificación para abrir el panel Definición de planificación estándar y planifique una operación de depuración.
8. Pulse Hecho para cerrar el panel.

Subir datos en una tabla personalizada

1. Abra el Creador de tablas personalizadas.
2. Elija una tabla personalizada pulsando el nombre de la tabla y resaltándola.
3. Pulse Subir datos para abrir el panel Importar datos.
4. En el recuadro Sentencia SQL, escriba una sentencia SQL válida para la tabla. El conjunto de resultados devuelto por la sentencia SQL debe tener la misma estructura que la tabla personalizada definida. Por ejemplo, si la tabla personalizada contiene todas las columnas de la tabla denominada my_table, escriba `select * from my_table`. Los siguientes campos, que son internos para Guardium, están disponibles para su uso en sentencias SQL:
   - ^FromDate?^ y ^ToDate?^ donde el valor es igual a la fecha de subida anterior y a la fecha de subida actual respectivamente.
   - ^fromID^ y ^toID^ donde, cuando se utilizan con Nombre de columna de ID constan del valor máximo de la columna de ID de la subida anterior y el valor máximo de la subida actual, respectivamente.

   Nota: No incluya ningún carácter de nueva línea en la sentencia SQL.
5. Especifique, si es necesario, un nombre de columna en el Nombre de columna de ID (de la tabla definida dentro del origen de datos) que se utilizará y que permitirá el seguimiento por ID y utilizarse junto con los campos de Guardium internos ^fromID^ y ^toID^.
6. En el mandato DML después del recuadro de subida, especifique un mandato DML (una sentencia SQL de actualización o supresión) sin punto y coma, para que se ejecute después de subir los datos. Nota: No incluya ningún carácter de nueva línea en la sentencia SQL.
7. Seleccione el recuadro Sobrescribir por subida si desea que los datos se depuren en la tabla personalizada antes de la subida. Marque la opción Sobrescribir por origen de datos si desea que los datos para ese origen de datos se depuren antes de realizar la subida.
8. Marque el botón de depuración predeterminado (en la pantalla Subir datos personalizados) como parte del objeto de depuración Trabajo de depuración de tabla personalizada predeterminado que tiene una antigüedad determinada inicial de 60 días. Para añadir una planificación de depuración para esta tabla, vaya a la página inicial Creador de tablas personalizadas, seleccione una tabla personalizada y pulse Depurar para abrir una pantalla de configuración Depurar datos de tabla personalizada.
9. Seleccione el recuadro Utilizar planificación predeterminada sólo si está subiendo tablas de versiones anteriores de Guardium. Este recuadro de selección solo aparece en una vista del Gestor central y solo para tablas personalizadas predefinidas Supervisor de uso de almacenamiento intermedio de CM, No tráfico empresarial, Cambios de S-TAP e Información de S-TAP.
10. Pulse Añadir origen de datos para abrir el Buscador de orígenes de datos en una ventana distinta. Utilice esta ventana para identificar una o más bases de datos desde las cuales se subirán los datos de la tabla. Puede añadir varios orígenes de datos para subirlos desde varios orígenes. Nota: Para un Gestor central, en la página Importación de datos hay un recuadro de selección de solo lectura denominado Incluir origen predeterminado. Si este recuadro de selección está marcado, la subida de datos se repetirá en todas las unidades gestionada registradas en línea. Nota: Cuando se añade un origen de datos, la aplicación no se puede planificar para que se ejecute sin especificar el nombre de usuario y la contraseña del origen de datos seleccionado.
11. Puede pulsar Comprobar/Reparar para comparar el esquema de la tabla personalizada con el esquema de los metadatos. Para entornos de gestión central: En un entorno de gestión central, la definición de tabla personalizada reside en el gestor central y puede que la tabla personalizada no exista en la base de datos local (unidad gestionada). Pulse el botón Comprobar/Reparar para comprobar si la tabla personalizada existe localmente y crear una si no existe.
12. Pulse Verificar orígenes de datos para probar la conexión de base de datos externa. Aparecerá una pantalla de confirmación.
13. Pulse Aplicar.

14. Para subir datos a esta tabla personalizada, realice una de las acciones siguientes:
    - Pulse Ejecutar una vez ahora para subir los datos manualmente.
    - Seleccione Modificar planificación para configurar la planificación.

Mantener tabla personalizada

Cuando siga el procedimiento para crear una tabla personalizada (detallado anteriormente) y seleccione una tabla personalizada predefinida, pulse Mantenimiento para gestionar el tipo de motor de tabla y el índice de tabla. Los tipos de motor de tabla para las tablas/titularidades personalizadas (InnoDB y MyISAM) aparecerán para todas las bases de datos personalizadas predefinidas porque los datos almacenados en la base de datos interna de Guardium están basados en MYSQL. Los dos tipos principales de motores de almacenamiento de tablas para bases de datos MySQL son InnoDB y MyISAM. Diferencias principales entre estos tipos de motor de tabla de MYSQL:

- InnoDB es más compleja mientras que MyISAM es más simple.
- InnoDB es más estricta en la integridad de los datos, mientras que MyISAM es más flexible.
- InnoDB implementa un bloqueo a nivel de fila para la inserción y actualización mientras que MyISAM implementa un bloqueo de nivel de tabla.
- InnoDB tiene transacciones mientras que MyISAM no tiene.
- InnoDB tiene restricciones de relaciones y claves foráneas mientras que MyISAM no tiene.

Nota: El cambio del tipo de motor no está permitido (y la selección aparece desactivada) si el número de fila de la tabla es mayor que 1M.

La otra selección en el menú Mantener tabla personalizada es Gestionar índice de tabla. Pulse Insertar para abrir Definición de índice de tabla. La pantalla emergente sugiere columnas en la tabla para añadir a índices basados en columnas utilizadas en dominios personalizados como condiciones de unión. Seleccione las columnas y guárdelas. Se crearán (o volverán a crear) los índices.

Planificar subidas de datos personalizados

Una vez que se ha establecido una definición de tabla personalizada, los datos se pueden subir a tablas personalizadas en el dispositivo Guardium de forma planificada.

Nota: Las instalaciones nuevas no inician automáticamente informes de empresa. Hay una planificación de subida para cada tabla personalizada. La cantidad total de espacio de disco reservado en el dispositivo de Guardium para las tablas personalizadas es de 4 GB.

1. Abra el Creador de tablas personalizadas.
2. Elija una tabla personalizada pulsando en la etiqueta de entidad y resáltela.
3. Pulse Subir datos para abrir el panel Importar datos.
4. Marque el recuadro de selección Utilizar planificación predeterminada para subir esta tabla utilizando la planificación predeterminada. De lo contrario, esta tabla personalizada utiliza su propia planificación de datos de subida.
5. Pulse Modificar planificación para abrir el panel Definición de planificación estándar y modifique la planificación.
6. Pulse Hecho cuando haya terminado.

La subida personalizada de los informes de empresa es igual que otros trabajos. Hay dos formas de habilitarlos:

- En la interfaz gráfica de usuario de subida de tabla personalizad. (Requiere licencia para la subida personalizada)
- Utilice GuardAPI desde la CLI:

```
grdapi add_schedule jobName=CustomTablePurgeJob_CM_SNIFFER_BUFFER_USAGE obGroup=customTableJobGroup Enterprise S-TAPs
Changed: grdapi add_schedule jobName=customTableDataUpload_106 jobGroup=customTableJobGroup CM Buffer Usage Monitor: grdapi
add_schedule jobName=customTableDataUpload_104 jobGroup=customTableJobGroup S-TAP Info: grdapi add_schedule
jobName=customTableDataUpload_80 jobGroup=customTableJobGroup
```

Crear un dominio personalizado

Después de definir una o más tablas personalizadas, defina un dominio personalizado para que pueda realizar tareas de consulta e informes utilizando los datos personalizados. La información recopilada se organiza en dominios, cada uno de los cuales contiene un tipo diferente de información relacionada con un área específica de interés: acceso a datos, excepciones, infracciones de política, etc. Existe una herramienta de creación de consultas independiente para cada dominio. Los dominios personalizados permiten dominios definidos por el usuario y pueden definir todas las tablas de datos subidas en el dispositivo de Guardium. Consulte Dominios personalizados. El uso para estos dominios de titularidad personalizados (privilegios) es para los informes de titularidad que se encuentran si se ha iniciado sesión como un usuario. Para ver estos informes, vaya al separador de usuario, DB Entitlements.

Nota: DB Entitlements Domains son componentes opcionales habilitados por clave de producto. Si estos componentes no se han habilitado, las opciones listadas en el tema de ayuda de Dominios personalizados no aparecerán en la selección del Creador de dominios personalizados.

1. Abra el Creador de dominios personalizados navegando a uno de lo siguiente:
    - Cumplir > Creación de informes personalizados > Creador de dominios personalizados
    - Informes > Herramientas de configuración de informes > Creador de dominios personalizados
    - Configurar > Herramientas y vistas > Creador de dominios personalizados
2. Pulse Dominios para abrir el panel Buscador de dominios.
3. Pulse Nuevo para abrir el panel Dominio de tablas personalizadas.
4. Escriba un Nombre de dominio. Normalmente, estará incluyendo una sola tabla personalizada en el dominio, por lo que es posible que desee utilizar el mismo nombre para el dominio.
5. El recuadro Entidades disponibles lista todas las tablas personalizadas que se han definido (y a las que tiene acceso). Seleccione una entidad. De forma opcional, pulse la herramienta (Filtro) para abrir el Filtro de entidades y especificar un valor Como para seleccionar solamente las entidades que desea que se listen y pulse Aceptar. Así se cerrará la ventana de filtro y volverá al panel Dominio de tablas personalizadas, con solo aquellas entidades que coincidan con el valor Como listado en el recuadro Entidades disponibles. Seleccione la entidad que desea incluir.
6. Pulse el botón de flecha > > para mover la entidad seleccionada en la lista Entidades disponibles a la lista Entidades de dominio.
7. Para añadir una entidad a un dominio que ya tiene una o más tablas, siga el procedimiento descrito. Necesitará utilizar la Condición de unión para definir la relación entre las entidades.

   Para cada entidad adicional:

    - En el recuadro Entidades de dominio, seleccione una entidad. Todos los atributos de dicha entidad pasarán a estar disponibles en la lista desplegable de campos del recuadro Entidades de dominio. Seleccione el atributo de esa lista que se utilizará en la operación de unión.
    - En la lista Entidades disponibles, seleccione la entidad que desea añadir. Todos los atributos de dicha entidad pasarán a estar disponibles en la lista desplegable de campos del recuadro Entidades disponibles. Seleccione el atributo de esa lista que se utilizará en la operación de unión.

- Seleccione = (el operador de igualdad) si desea que la condición de unión sea igual (por ejemplo, domainA.attributeB = domainC.attributeD). Seleccione una unión externa si desea que la condición de unión sea una unión externa utilizando los atributos seleccionados.
- Pulse Añadir pareja de campos. Añadir pareja de campos se puede utilizar para añadir más pares de atributos de estas dos entidades a la condición de unión.
- Repita los pasos para las operaciones de unión adicionales.

Nota: Cuando la seguridad a nivel de datos está activada, las entidades internas añadidas al dominio personalizado no pueden pertenecer a dominios diferentes con políticas de filtrado.

8. Seleccione el atributo Indicación de fecha y hora para la entidad de dominio personalizado.
   Nota: Se debe utilizar al menos una entidad con una indicación de fecha y hora, ya que es necesaria una indicación de fecha y hora para guardar un dominio personalizado.
9. Pulse Aplicar.

Modificar un dominio personalizado

El objetivo es crear un enlace entre los datos externos y los datos internos.

1. Abra el Creador de dominios personalizados.
2. Elija el Dominio personalizado que desea clonar
3. Pulse Modificar para abrir el panel Dominio de tablas personalizadas.
4. Consulte Abra el Creador de dominios personalizados y Enlazar datos externos con datos internos para obtener ayuda.
5. Pulse Aplicar para guardar los cambios.

Eliminar un dominio personalizado

1. Abra el Creador de dominios personalizados.
2. Elija el Dominio personalizado que desea clonar.
3. Pulse Dominios para abrir el panel Buscador de dominios.
4. Pulse Suprimir para eliminar el dominio personalizado.

Clonar un dominio personalizado

1. Abra el Creador de dominios personalizados.
2. Elija la Tabla personalizada que está en el dominio que desea clonar.
3. Pulse Dominios para abrir el panel Buscador de dominios.
4. Pulse Clonar para abrir el panel Dominio de tablas personalizadas.
5. Cambie el Nombre de dominio para que refleje el nuevo dominio.
6. Consulte Abra el Creador de dominios personalizados y Enlazar datos externos con datos internos para obtener ayuda.
7. Pulse Aplicar para guardar los cambios.

Enlazar datos externos con datos internos

El objetivo es crear un enlace entre los datos externos y los datos internos.

1. Abra el Creador de dominios personalizados.
2. Elija la Tabla personalizada que tiene los datos externos.
3. Pulse Dominios para abrir el panel Buscador de dominios.
4. Pulse Modificar para abrir el panel Dominio de tablas personalizadas.
5. Pulse el icono Filtro junto a las Entidades disponibles.
6. Deseleccione el recuadro Personalizado para el filtro y, opcionalmente, rellene una condición Como para filtrar los nombres de entidad y pulse Aceptar.
7. Seleccione una entidad en las Entidades disponibles que le gustaría enlazar con los datos externos.
8. Seleccione el campo que se utilizará para unir datos con los datos externos.
9. Resalte la tabla de las Entidades de dominio que contiene los datos externos.
10. Seleccione el campo que se utilizará para unir datos con los datos internos.
11. Pulse Añadir pareja de campos para añadir la relación.
12. Pulse la flecha doble > > para añadir la tabla interna a la lista Entidades de dominio.
13. Pulse Aplicar para guardar los cambios.

Cómo trabajar con consultas personalizadas

Esta sección describe cómo abrir el Creador de consultas personalizadas. Consulte Creación de consultas y Creación de informes para obtener ayuda para definir una consulta y crear un informe. Utilice el Creador de consultas personalizadas para crear consultas a partir de datos de dominios personalizados, que contienen una o más tablas personalizadas.

1. Abra el Creador de consultas personalizadas navegando a Cumplir > Creación de informes personalizados > Creador de consultas personalizadas.
2. Seleccione un dominio amperio en la lista.
3. Pulse Buscar para abrir el Buscador de consultas
4. Para ver, modificar o clonar una consulta existente, selecciónela en la lista Nombre de consulta o seleccione un informe utilizando dicha consulta en la lista Título de informe.
5. Para ver todas las consultas definidas para una tabla personalizada específica, seleccione dicha tabla personalizada en la lista Entidad principal y pulse el botón Buscar (solo se listarán las tablas personalizadas incluidas en el dominio personalizado seleccionado).

Interfaz bidireccional hacia o desde InfoSphere Discovery

Tanto IBM Guardium como InfoSphere Discovery tienen la capacidad de identificar y clasificar datos confidenciales como, por ejemplo, números de seguridad social o números de tarjetas de crédito.

Un cliente del producto IBM Guardium puede utilizar una interfaz bidireccional para transferir información de datos confidenciales identificada de un producto a otro. Aquellos clientes que ya han invertido el tiempo en un producto de InfoSphere pueden transferir la información al otro producto de InfoSphere.
Nota: En IBM Guardium, el proceso de clasificación es un proceso en curso que se ejecuta periódicamente. En InfoSphere Discovery, la clasificación forma parte del proceso de descubrimiento que normalmente se ejecuta una vez.

Los datos se transferirán a través de archivos CSV.

El resumen de los procedimientos de exportación/importación es el siguiente:

- Exportar de Guardium: Ejecutar el informe predefinido (Exportación de datos confidenciales a descubrimiento) y exportar como archivo CSV.
- Importar a Guardium: Subir a una tabla personalizada en el origen de datos CSV; definir el informe predeterminado para este origen de datos.

Siga estos pasos:

- Exportar de Guardium
- Exportar datos de clasificación de IBM Guardium a InfoSphere Discovery

1. Como usuario administrador en la aplicación Guardium, vaya a Herramientas > Creación de informes > Seguimiento de resultados de clasificador > Seleccionar un informe > Exportar datos confidenciales a descubrimiento.
   Nota: Añada este informe al panel de la interfaz de usuario (no es así de forma predeterminada).
2. Pulse el icono Personalizar en la pantalla Resultado de informe y especifique los criterios de búsqueda para filtrar los datos de resultados de clasificación para transferir a Descubrimiento.
3. Ejecute el informe y pulse Bajar todos los registros.
4. Guarde como CSV e importe este archivo a Discovery según las Instrucciones de InfoSphere Discovery.

Importar a Guardium

Importar datos de clasificación de InfoSphere Discovery a IBM Guardium

1. Exporte los datos de clasificación como CSV desde InfoSphere Discovery basándose en las instrucciones de InfoSphere Discovery.
2. Abra el Creador de tablas personalizadas navegando a uno de lo siguiente:
   - Cumplir > Creación de informes personalizados > Creador de tablas personalizadas
   - Informes > Herramientas de configuración de informes > Creador de tablas personalizadas

   Seleccione ClassificationDataImport y pulse Subir datos.
3. En la pantalla Subir datos, pulse Añadir origen de datos, pulse Nuevo, defina el archivo CSV importado de Discovery como nuevo origen de datos (Tipo de base de datos = Texto).
   Nota: De forma alternativa, puede subir los datos directamente desde la base de datos de Discovery si sabe cómo acceder a la base de datos de Discovery y a los datos de resultados de clasificación.
4. Después de definir el archivo CSV como origen de datos, pulse Añadir en la pantalla de lista de orígenes de datos.
5. En la pantalla Subir datos, pulse Verificar origen de datos y, a continuación, Aplicar.
6. Pulse Ejecutar una vez ahora para subir los datos desde el CSV.
7. Vaya a Creador de informes, seleccione el informe Importación de datos de clasificación, pulse Añadir al panel para añadirlo al Portal y, a continuación, vaya al informe.
8. Acceda al informe, pulse Personalizar para establecer las fechas de inicio y fin, y ejecuta el informe.

El resultado del informe tiene los datos de clasificación importados de InfoSphere Discovery. Efectúe una doble pulsación para invocar las API asignadas a este informe. Los datos importados de Discovery pueden utilizarse para lo siguiente:

- Añadir nuevo origen de datos basado en el conjunto de resultados.
- Añadir/Actualizar grupo de datos confidenciales.
- Añadir reglas de política basadas en detalles de datos de origen de datos y confidenciales.
- Añadir conjunto de privacidad.

Firma de interfaz de CSV

Utilice la tabla para ver ejemplos de firmas de interfaz de CSV utilizadas en la transferencia bidireccional entre IBM Guardium e InfoSphere Discovery.

Tabla 2. Firma de interfaz de CSV

Firma de interfaz	Ejemplo
Tipo	DB2
Host	9.148.99.99
Puerto	50001
dbName (Nombre de esquema para DB2 u Oracle, nombre de base de datos para otros)	cis_schema
URL de origen de datos	
TableName	MK_SCHED
ColumnName	ID_PIN
ClassificationName	SSN
RuleDescription	Algoritmo predefinido de InfoSphere Discovery
HitRate	70% - no disponible para exportar en Guardium Vers. 8.2
ThresholdUsed	60% - no disponible para exportar a Guardium Vers. 8.2

Tema principal: Supervisar y auditar

Conjuntos de privacidad

Un conjunto de privacidad es un conjunto de elementos que se pueden utilizar para realizar una supervisión especial.

Consta de uno o varios pares objeto-campo, por ejemplo, el campo de salario de la tabla de empleados, o todos los campos de la tabla de historial de salarios. Se puede informar de todos los accesos a estos elementos dentro de un periodo de tiempo determinado.

Seleccione cualquiera de los temas para trabajar con conjuntos de privacidad.

Abrir el Creador de conjuntos de privacidad

Para acceder a la definición del conjunto de la privacidad, a la cuenta de usuario de Guardium se le debe asignar un rol de seguridad que también esté asignada a esa definición del conjunto de la privacidad. Los conjuntos de privacidad a los que no puede acceder no se visualizarán en una lista de conjuntos de privacidad.

1. Abra el panel Identificar conjunto de privacidad navegando a uno de los siguientes:
   - Cumplir > Herramientas y vistas > Creador de conjuntos de privacidad
   - Descubrir > Descubrimiento de base de datos > Creador de conjuntos de privacidad
2. Realice una de las siguientes acciones:
   - Pulse el botón Nuevo para definir un conjunto de privacidad nuevo (consulte Crear conjunto de privacidad).
   - Seleccione un conjunto de privacidad de la lista y pulse uno de los botones siguientes:
     - Clonar: Consulte Clonar un conjunto de privacidad.
     - Modificar: Utilice este botón para modificar la definición o para ejecutar un informe basado en esa definición. Consulte Modificar un conjunto de privacidad, o Ejecutar un informe de conjunto de privacidad.
     - Eliminar: consulte Eliminar un conjunto de privacidad.

Crear un conjunto de privacidad

1. Abra el panel Identificar conjunto de privacidad navegando a uno de los siguientes:
   - Cumplir > Herramientas y vistas > Creador de conjuntos de privacidad
   - Descubrir > Descubrimiento de base de datos > Creador de conjuntos de privacidad
2. Pulse Nuevo para abrir el panel Definición del conjunto de privacidad.
3. En el recuadro Descripción del conjunto de privacidad, especifique un nombre exclusivo para el conjunto de privacidad. No incluya caracteres de apóstrofo en el nombre. Este es el nombre que se visualizará en el panel Identificar conjunto de privacidad.
4. En la lista desplegable Clasificación de seguridad, seleccione opcionalmente una clasificación de seguridad para este conjunto de privacidad.
5. En el panel Elementos de este panel Conjunto de privacidad, para cada par de elementos que se van a incluir:
   - Especifique un nombre en el recuadro Objeto.
   - Especifique un nombre de campo en el cuadro Campo, o marque el recuadro Cualquier campo de este objeto para incluir todos los campos contenidos en el objeto especificado.
   - Pulse Añadir este nuevo par Objeto - Campo.
6. Cuando se hayan añadido todos los elementos, pulse Guardar.
7. Opcionalmente, pulse el botón Roles para añadir roles.
8. Opcionalmente, pulse el botón Comentarios para añadir comentarios.

Modificar un conjunto de privacidad

1. Abra el conjunto de privacidad que se va a modificar en el Creador de conjuntos de privacidad. Consulte Abrir el Creador de conjuntos de privacidad.
2. Realice los cambios en la definición del conjunto de privacidad, según sea necesario. Para obtener una descripción de todos los campos, consulte Crear un conjunto de privacidad.
3. Pulse Guardar.
4. Pulse Hecho cuando haya terminado.

Clonar un conjunto de privacidad

1. Abra el conjunto de privacidad que se va a clonar en el Creador de conjuntos de privacidad. Consulte Abrir el Creador de conjuntos de privacidad.
2. El conjunto de privacidad clonado se denominará "Copia de" conjunto de privacidad seleccionado. Recomendamos cambiarlo por algo más significativo. No incluya caracteres de apóstrofo en el nombre.
3. Realice los cambios adicionales en la definición del conjunto de privacidad, según sea necesario. Para obtener una descripción de todos los campos, consulte Crear un conjunto de privacidad.
4. Pulse Guardar.
5. Pulse Hecho cuando haya terminado.

Eliminar un conjunto de privacidad

Si se está ejecutando un proceso de auditoría, no puede eliminar un conjunto de privacidad. Detenga el proceso de auditoría y, a continuación, siga los pasos para eliminar el conjunto de privacidad.

1. Seleccione el conjunto de privacidad que se va a eliminar, en el panel Identificar conjunto de privacidad. Consulte Abrir el Creador de conjuntos de privacidad.
2. Pulse Suprimir y confirme la acción.
3. Pulse Hecho.

Ejecutar un conjunto de privacidad

Este procedimiento describe cómo ejecutar un informe de conjunto de privacidad bajo demanda. Para planificar un informe de conjunto de privacidad, inclúyalo en un flujo de trabajo de conformidad (consulte Automatización de flujo de trabajo de cumplimiento).

1. Abra el conjunto de privacidad para el informe en el Creador de conjuntos de privacidad. Consulte Abrir el Creador de conjuntos de privacidad.
2. Pulse Ejecutar.
3. En los Parámetros de tarea, especifique la hora de inicio y finalización para la tarea.
4. Seleccione Informar por detalles de acceso o Informar por usuario de aplicación para especificar cómo deben visualizarse los resultados. La primera opción es el valor predeterminado, en cuyo caso se muestra un recuento de accesos para cada combinación de IP de cliente, IP de servidor, servidor (nombre), tipo de servidor, protocolo de base de datos, nombre de programa fuente y nombre de usuario de base de datos. Si se selecciona Usuario de aplicación, el informe contendrá una columna aparte con ese nombre (después Nombre de usuario de BD) y la salida estará calificada adicionalmente por el usuario de la aplicación.
5. Pulse Ejecutar una vez ahora. Una vez que se ha ejecutado el informe, se visualizará en una ventana distinta.
6. Pulse Hecho.

Tema principal: Supervisar y auditar

Alertas personalizadas

Los mensajes de alerta se pueden distribuir a través de correo electrónico, SNMP, syslog o clases Java™ escritas por el usuario. La última opción se conoce como alerta personalizada.

Cuando se desencadena una alerta, una clase de alerta personalizada puede realizar cualquier acción adecuada para la situación; por ejemplo, puede actualizar una página web o enviar un mensaje de texto a un número de teléfono.

Para crear una clase de generación de alertas personalizada, primero póngase en contacto con el servicio de soporte técnico para obtener el archivo de interfaz necesario. En el tema siguiente se describe cómo implementar la interfaz. Consulte Utilizar la interfaz de alertas personalizadas así como el tema siguiente, que contiene un ejemplo: Clase de alertas personalizadas de ejemplo.

Una vez que se ha compilado la clase, se debe subir en el dispositivo de Guardium. Consulte Gestionar clases personalizadas.

Para obtener directrices sobre cómo probar una clase de alertas personalizadas, consulte la sección Probar una clase de alerta personalizada más adelante en este tema.

Nota: No obtenga ni ejecute código personalizado de orígenes de datos no de confianza para reducir el riesgo de vulnerabilidades de seguridad.
Nota: No obtenga ni ejecute código personalizado de orígenes no de confianza.
Nota: No escriba una clase personalizada que obtenga datos de un origen no de confianza.

Utilizar la interfaz de alertas personalizadas

La clase de alertas personalizadas debe estar en el paquete com.guardium.custom y deben implementar la interfaz com.guardium.custom.alerts.CustomerDefinedAlertingIfc:

```
package com.guardium.custom
public class YourClassNameHere implements CustomerDefinedAlertingIfc {
       }
```

La interfaz contiene los cinco métodos descritos.

Tabla 1. Método processAlert

Método 1	
Descripción	Procesar un solo mensaje de alerta.
Sintaxis	public void processAlert (String message, Date timeStamp)
Parámetros	Una serie que contiene el mensaje generado por la alerta. Se ha creado un java.util.Date para la hora del mensaje de alerta.

Tabla 2. Método getMessage

Método 2	
Descripción	Devolver el mensaje de alerta
Sintaxis	public String getMessage ()
Parámetros	Una serie que contiene el mensaje de alerta.

Tabla 3. Método getTimeStamp

Método 3	
Descripción	Devolver la indicación de fecha y hora asociada al mensaje de alerta.
Sintaxis	public Date getTimeStamp ()
Parámetros	Se ha creado un java.util.Date para la hora del mensaje de alerta.

Tabla 4. Método setMessage

Método 4	
Descripción	Establecer el mensaje de alerta.
Sintaxis	public void setMessage (String inMessage)
Parámetros	Una serie que contiene el mensaje de alerta.

Tabla 5. Método setTimeStamp

Método 5	
Descripción	Establecer la indicación de fecha y hora asociada con el mensaje de alerta.
Sintaxis	public void setTimeStamp (Date inDate)
Parámetros	Se ha creado un java.util.Date para la hora del mensaje de alerta.

Clase de alertas personalizadas de ejemplo

El programa de ejemplo siguiente implementa los cinco métodos descritos en la sección anterior. Para el método processAlert, este programa simplemente escribe el mensaje de alerta y la indicación de fecha y hora en la consola del sistema.

```
/*
 * Clase de alertas personalizadas de ejemplo
 *
 */
package com.guardium.custom;
import java.text.DateFormat;
import java.util.Date;
public class HandleAlerts implements CustomerDefinedAlertingIfc {
```

```
private String message = "";
private Date timeStamp = null;
public void processAlert(String message, Date timeStamp){
setMessage(message);
setTimeStamp(timeStamp);
System.out.println(getMessage() + " on " +
  DateFormat.getDateInstance(). format(getTimeStamp()));
}
    public void setMessage(String inMessage){
        message = inMessage;
    }
    public String getMessage(){
        return message;
    }
    public void setTimeStamp(Date inDate){
        timeStamp = inDate;
    }
    public Date getTimeStamp(){
        return timeStamp;
    }
}
```

Probar una clase de alerta personalizada

Después de compilar una clase de alertas personalizadas, siga el procedimiento para probarla.

1. Suba la clase personalizada al dispositivo. Se trata de una función de administración que se realiza desde la consola de administrador. Consulte Gestionar clases personalizadas.
2. Defina una alerta de correlación o en tiempo real para utilizar la clase de alerta personalizada. Independientemente del tipo de alerta que genere la alerta, la prueba es más fácil si asigna un segundo tipo de notificación (por ejemplo, correo electrónico) con el que poder comparar los resultados de alertas personalizadas.
3. Compruebe el entorno realizando una de las acciones siguientes:
    - Para una alerta de correlación:
        - Compruebe que el intervalo de sondeo de detección de anomalías es adecuado para las pruebas y que se ha iniciado la detección de anomalías. Si el intervalo de sondeo es demasiado largo (puede ser de 30 minutos o más), es posible que haya un intervalo de espera largo antes de que se ejecute la consulta.
        - Compruebe que el intervalo de sondeo del Alertador es adecuado para la realización de pruebas y que se ha iniciado el Alertador.
        - Compruebe que la alerta que se va a probar se haya marcado como Activa.
    - Para una alerta en tiempo real:
        - Compruebe que la política que contiene la regla con la acción de alerta personalizada. es la política instalada.
        - Verifique que el motor de inspección se haya reiniciado después de instalar la política actualizada.
        - Compruebe que el intervalo de sondeo de Alertador es adecuado para la realización de pruebas y que se ha iniciado.
4. Lleve a cabo cualquier acción que sea necesaria para desencadenar la alerta (por ejemplo, generar una serie de anomalías de inicio de sesión).

Tema principal: Supervisar y auditar

Proceso Flat Log

La opción Flat Log es un proceso para permitir que el dispositivo de Guardium registre información sin analizarla inmediatamente en tiempo real.

Esto ahorra recursos de proceso, para que se pueda manejar un volumen de tráfico más elevado. El análisis y la amalgama de esos datos en la base de datos interna de Guardium se pueden realizar más adelante, ya sea en un recopilador o en una unidad de agregador.

Nota: Las reglas para proceso flat no funcionan con reglas de política que involucran a un campo, un objeto, un verbo SQL (mandatos), un grupo de mandatos/objetos y un grupo de campos/objetos. En el proceso Flat Log, "flat" significa que no se crea el árbol de sintaxis. Si no hay ningún árbol de sintaxis, los campos, objetos y verbos SQL no se pueden determinar.

Las acciones siguientes no funcionan con reglas en políticas flat: REGISTRAR TODOS LOS DETALLES; REGISTRAR TODOS LOS DETALLES POR SESIÓN; REGISTRAR TODOS LOS DETALLES CON VALORES; REGISTRAR TODOS LOS DETALLES POR SESIÓN; REGISTRAR DETALLES DE ENMASCARAMIENTO.

La selección de esta característica incluye el menú de Creador de políticas en el menú Configuración > Herramientas y vistas y Proceso Flat Log en Gestionar > Supervisión de actividad.

Cuando la opción del recuadro de selección Registro para proceso flat (Flat Log) listada en la pantalla Definición de política del Creador de políticas está marcada,

- Los datos no se analizarán en tiempo real.
- Los flat log pueden verse en un informe de Lista de Flat Log designada.

1. Vaya a Gestionar > Supervisión de actividad > Proceso Flat Log.
2. Seleccione la actividad a realizar:
    - Proceso: Fusionar la información de flat log para la base de datos interna.
    - Archivador/Agregación/Depuración: Archivar o agregar, y opcionalmente depurar, el flat log.
    - Sólo depurar: Depurar los datos de flat log.
3. Pulse Aplicar para guardar la configuración.
4. Para una actividad de proceso, realice una de las acciones siguientes:
    - Pulse Ejecutar una vez ahora para fusionar inmediatamente la información de flat log con la base de datos interna.
    - Pulse Modificar planificación para definir una planificación para esta actividad. Puede seleccionar la hora de inicio, la frecuencia de reinicio y la frecuencia de repetición. Para el campo Planificar por.., debe seleccionar Día/Semana o Meses. Consulte Planificación para obtener más información sobre la planificación.

Tema principal: Supervisar y auditar

Crear expresión en condición de consulta

Utilice el icono Añadir expresión, junto a las selecciones Valor, Parámetro, Atributo, para especificar las Condiciones de consulta, incluidas las expresiones matemáticas y las series definidas por el usuario.

Utilice esta característica cuando necesite añadir una condición que no esté basada en todo el contenido del atributo tal cual, sino en parte del atributo, una función del atributo o una función que combine más de un atributo.

Un ejemplo es: `INSTR(:attribute, '150.1') = 5`, que devolverá todas las instancias de IP de cliente que coincidan con los cinco caracteres listados. Escriba el carácter 5 en el recuadro de entrada situado junto al icono Añadir expresión. Escriba la expresión `INSTR(:attribute, '150.1')` en la ventana Crear expresión independiente. Pruebe la validez de la expresión en la ventana Crear expresión. Otro ejemplo es: `LENGTH(:attribute) >= 40`, que devolverá la longitud de cualquier sentencia SQL superior a 40 caracteres. La expresión puede (o no puede) contener referencias al atributo real y también puede contener referencias a otros atributos.

Tema principal: Supervisar y auditar

Informes de titularidad de base de datos

Las revisiones de titularidad son el proceso de validación y garantía de que los usuarios solo tienen los privilegios necesarios para llevar a cabo sus tareas.

Junto con la autenticación de usuarios y la restricción de privilegios de acceso basados en roles a los datos, incluso para los usuarios de bases de datos con más privilegios, existe la necesidad de realizar revisiones de derechos periódicamente, el proceso de validación y garantizar que los usuarios sólo tengan los privilegios necesarios para realizar sus tareas. Esto también se conoce como informe de certificación de derechos de usuario de base de datos.

Utilice los informes de titularidad (privilegio) de base de datos predefinidos de Guardium (por ejemplo) para ver quién tiene privilegios de sistema y quién ha otorgado estos privilegios a otros usuarios y roles. Los informes de titularidad de base de datos son importantes para los auditores que realizan seguimientos de los cambios en el acceso a la base de datos y para garantizar que no existen los agujeros de seguridad de cuentas persistentes o privilegios mal otorgados.

Se han creado informes de titularidad de base de datos personalizados para ahorrar tiempo de configuración y facilitar la subida y el informe de datos de las siguientes bases de datos: Oracle; MYSQL; DB2; SYBASE; SYBASE IQ; Informix; MS SQL 2000/2005/2008; Netezza; Teradata; y, PostgreSQL; DB2 en z/OS.

Para bases de datos Microsoft SQL Server y Oracle, también puede utilizar Optimización de titularidades para acceder a esta información.

Siga estos pasos para utilizar los informes de titularidad de base de datos predefinidos (privilegio) de Guardium con instantáneas actualizadas de usuarios de bases de datos y privilegios de acceso:

1. Añada orígenes de datos/bases de datos al dispositivo (vaya a Cumplir > Creación de informes personalizados > Creador de dominios personalizados.
2. Asigne los orígenes de datos a las titularidades (vaya a Cumplir > Creación de informes personalizados > Creador de tablas personalizadas. Seleccione la lista de tablas personalizadas de su titularidad. Pulse Subir datos. Asigne orígenes de datos al informe de titularidad en la pantalla del menú Importar datos. Cuando haya terminado, pulse Ejecutar una vez ahora.
3. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador Titularidades de BD.

Los informes de titularidad de BD utilizan la característica Dominio personalizado de Guardium para crear enlaces entre los datos externos en la base de datos seleccionada con los datos internos de los informes de titularidad predefinidos. Consulte Correlación de datos externos para obtener más información sobre el Creador de dominios personalizados/Creador de consultas personalizadas/Creador de tablas personalizadas.

Los informes de titularidad predefinidos se listan en Informes de titularidad de base de datos.

Tema principal: Supervisar y auditar

Identificación de usuario

Guardium proporciona varios métodos para identificar a los usuarios de la aplicación, cuando el usuario de la base de datos no es evidente a partir del tráfico de la base de datos.

Algunas aplicaciones de base de datos se han diseñado para utilizar o compartir un pequeño número de cuentas de usuario de base de datos. Estas aplicaciones gestionan sus usuarios independientemente del sistema de gestión de base de datos, lo que significa que al observar tráfico de base de datos desde fuera de la aplicación, puede ser difícil determinar el usuario de la aplicación que está controlando una conexión de base de datos en cualquier momento. Sin embargo, cuando se producen actividades de base de datos cuestionables, es necesario relacionar acciones específicas con individuos específicos, en lugar de hacerlo con una cuenta compartida por grupos de personas. En otras palabras, debe conocer el usuario de la aplicación, no solo el usuario de la base de datos.

Guardium proporciona varios métodos para identificar a los usuarios de la aplicación, cuando el usuario de la base de datos no es evidente a partir del tráfico de la base de datos:

- Identificar usuarios a través de la conversión de usuarios de aplicación: Para algunas de las aplicaciones comerciales más populares (Oracle EBS, PeopleSoft, SAP, etc.), Guardium puede identificar a los usuarios automáticamente.
- Identificar usuarios mediante API: La API de sucesos de aplicación permite indicar a Guardium cuando un usuario de la aplicación toma o cede el control de una conexión, o cuando se produce cualquier otro suceso de interés. (Esto se puede utilizar para más de solo identificar usuarios).
- Identificar usuarios a través de procedimientos almacenados: Muchas aplicaciones utilizan procedimientos almacenados de base de datos para identificar el usuario de aplicación. En estos casos, normalmente la información de usuario se puede extraer de los parámetros de procedimientos almacenados.

En la empresa, es posible que sea necesario emplear varios métodos para identificar usuarios, en función de las aplicaciones utilizadas.

- Identificar usuarios a través de la conversión de usuarios de aplicación
  Algunas aplicaciones gestionan una agrupación de conexiones de base de datos. En estas arquitecturas de tres niveles, todas las conexiones agrupadas inician sesión en una base de datos utilizando un único ID funcional y, a continuación, gestionan internamente todos los usuarios de la aplicación. Cuando una sesión de usuario necesita acceso a la base de datos, adquiere una conexión de la agrupación, la utiliza y, a continuación, la libera de nuevo a la agrupación. Cuando esto sucede, Guardium puede ver cómo interactúa la aplicación con la base de datos, pero no puede atribuir acciones de base de datos específicas a usuarios específicos de la aplicación.
- Identificar usuarios mediante API
  Para algunas aplicaciones que gestionan usuarios internamente, el usuario de la aplicación no se puede identificar desde el tráfico. Cuando esto sucede, puede utilizar la API de sucesos de aplicación de Guardium.
- Identificar usuarios a través de procedimientos almacenados
  En muchas aplicaciones existentes, toda la información necesaria para identificar un usuario de la aplicación puede obtenerse del tráfico de la base de datos existente, a partir de las llamadas de procedimientos almacenados. Una vez que Guardium sabe qué llamadas hay que vigilar y qué parámetros contienen el nombre de usuario u otra información de interés, los usuarios se pueden identificar automáticamente.

Tema principal: Supervisar y auditar

Identificar usuarios a través de la conversión de usuarios de aplicación

Algunas aplicaciones gestionan una agrupación de conexiones de base de datos. En estas arquitecturas de tres niveles, todas las conexiones agrupadas inician sesión en una base de datos utilizando un único ID funcional y, a continuación, gestionan internamente todos los usuarios de la aplicación. Cuando una sesión de usuario necesita acceso a la base de datos, adquiere una conexión de la agrupación, la utiliza y, a continuación, la libera de nuevo a la agrupación. Cuando esto sucede, Guardium puede ver cómo interactúa la aplicación con la base de datos, pero no puede atribuir acciones de base de datos específicas a usuarios específicos de la aplicación.

Para algunas aplicaciones ampliamente utilizadas, Guardium tiene soporte incorporado para identificar la información de usuario final de la aplicación y, por lo tanto, puede relacionar la actividad de la base de datos con los usuarios finales de la aplicación.

Para utilizar este recurso, siga estos procedimientos:

1. Defina una configuración de conversión de usuarios de aplicación para la aplicación. Consulte Configurar la detección de usuarios de aplicación.
2. Rellene cualquier grupo predefinido necesario para dicha aplicación. Consulte Rellenar grupos de aplicaciones definidos previamente.
3. Vuelva a generar todos los portlets para informes especiales para esa aplicación y coloque los portlets en una página. Consulte Regenerar portlets de informes de aplicaciones especiales.

Seguimiento de auditoría selectivo y Conversión de usuarios de aplicación

Si la política de acceso a datos instalada utiliza la característica de seguimiento de auditoría selectivo para limitar la cantidad de datos registrados, hay dos consideraciones importantes que se aplican a la conversión de usuarios de aplicación:

- La política ignorará todo el tráfico que no se ajuste al rol de conversión de usuarios de aplicación (por ejemplo, no desde el servidor de aplicaciones).
- Solo el SQL que coincida con el patrón para dicha política de seguridad estará disponible para los informes de conversión de usuarios de aplicación.

Configurar la detección de usuarios de aplicación

1. Vaya a Proteger > Detección de intrusión en base de datos > Conversión de usuarios de aplicación. Los detalles para las configuraciones de conversión de usuarios de aplicación existentes se muestran en la parte superior de la página.
2. Empiece a crear una nueva configuración de conversión de usuarios de aplicación especificando un código exclusivo en el recuadro Código de aplicación.
   Nota: En Gestión central, debe utilizar códigos de aplicación diferentes en máquinas gestionadas diferentes. Esto impide que los alias generados para los usuarios entren en conflicto entre sí. (En Gestión central, hay un conjunto de alias compartido por todas las unidades gestionadas).
3. En la lista Tipo de aplicación, seleccione el tipo de aplicación:
   - BO-WI - Business Objects / Web Intelligence
   - EBS - Oracle E-Business Suite
   - PeopleSoft
   - SAP Observed
   - SAP DB
   - SIEBEL Observed
   - SIEBEL DB
4. En el recuadro Versión de aplicación, especifique el número de versión de la aplicación (por ejemplo, 11).
5. En la lista Tipo de base de datos, seleccione el tipo de base de datos. Sólo se visualizarán los tipos que están disponibles para el tipo y la versión de aplicación seleccionados.
   Nota: Cuando el Tipo de aplicación se establece en EBS, SIEBEL DB o SAP DB, tiene la opción de seleccionar entre orígenes de datos preexistentes pulsando el botón Añadir origen de datos. El origen de datos debe coincidir con uno de los tipos de base de datos soportados para el tipo de aplicación que se está configurando.
6. En el recuadro IP de servidor, especifique la dirección IP que utiliza la aplicación para conectarse a la base de datos.
7. En el recuadro Puerto, especifique el número de puerto que utiliza la aplicación para conectarse a la base de datos.
8. En el recuadro Nombre de instancia, especifique el nombre de instancia que utiliza la aplicación para conectarse a la base de datos.
9. En el recuadro Nombre de BD, especifique el nombre de base de datos para la aplicación. (Es necesario para algunas aplicaciones, no se utiliza para otras).
10. Marque el recuadro Activo para habilitar la conversión de usuarios. Nada se convierte hasta después de la primera importación de definiciones de usuario.
11. Especifique un nombre de usuario para Guardium para utilizarlo al acceder a la base de datos. Especifique una contraseña para Guardium para utilizarla al acceder a la base de datos.
12. Marque el recuadro Responsabilidad si desea asociar las responsabilidades (por ejemplo, Administración) con nombres de usuario. También puede deseleccionar el recuadro Responsabilidad para simplemente registrar nombres de usuario. Cuando el recuadro está deseleccionado, todas las actividades realizadas por un usuario se agruparán juntas, independientemente de la responsabilidad que haya en el momento en que se ha producido la actividad.
    Nota: Si el tipo de aplicación es EBS (el tipo de base de datos es Oracle), aparecerán dos opciones adicionales: Conectar a IP de servidor y Conectar a nombre de usuario. Si se rellena, el sistema se conectará utilizando dicha dirección IP y nombre de usuario para recuperar los nombres de usuario y la responsabilidad.
13. Pulse el botón Añadir para guardar la definición de Conversión de usuarios de aplicación.
14. Continúe con los procedimientos: Rellenar grupos de aplicaciones definidos previamente y Regenerar portlets de informes de aplicaciones especiales.
15. Después de realizar el paso anterior, vaya a Gestionar > Supervisión de actividad > Motores de inspección y pulse Reiniciar motores de inspección en el panel Configuración de motor de inspección.
16. Después de realizar las tareas especificadas en los dos procedimientos del paso 16, vuelva a Conversión de usuarios de aplicación y pulse Ejecutar una vez ahora para importar las definiciones de usuario para esta aplicación (y cualquier otra definida).
17. Más adelante, después de verificar que la operación de importación de datos ha funcionado satisfactoriamente (consulte el paso 20), vuelva a este panel y pulse el botón Modificar planificación para definir una operación de importación para que se ejecute periódicamente. Debe planificar la importación de datos de definición de usuario en cualquier intervalo que sea adecuado para su entorno. El tiempo máximo que un nombre de usuario de aplicación nuevo no estará disponible es el tiempo entre las ejecuciones de la operación de importación. Para obtener instrucciones detalladas sobre cómo utilizar el planificador, consulte Planificación.
18. La importación de datos de Conversión de usuarios de aplicación puede confirmarse examinando informes predefinidos, por ejemplo, Acceso a la aplicación de SAP. Vaya a Informes > Herramientas de configuración de informes > Creador de informes y elija el informe Acceso a la aplicación de SAP. Vuelva a generar este informe y añádalo a un panel y, a continuación, establezca el rango de fechas en un valor bastante grande (por ejemplo, retroceda un año para los datos).

Nota: La primera vez que se pulsa Ejecutar una vez ahora después de instalar los valores de Conversión de usuarios de aplicación, se recupera la última fecha de actualización para las tablas que se examinan. Después de eso, solo importa datos nuevos. De lo contrario, nos podríamos encontrar importando décadas de datos y llenando muchas tablas y bases de datos.

Rellenar grupos de aplicaciones definidos previamente

Cuando se ha configurado la Conversión de usuarios de aplicación, debe rellenar al menos dos grupos predefinidos con información que será específica del entorno. Esta tabla identifica los grupos que deben rellenarse para cada tipo de aplicación. Para obtener instrucciones sobre cómo cumplimentar un grupo, consulte Visión general de

grupos.

Aplicación	Grupo predefinido	Tipo de grupo
EBS	Servidores de aplicaciones EBS	IP de cliente
	Servidores de BD de EBS	IP de servidor
PeopleSoft	Servidores de aplicaciones PSFT	IP de cliente
	Servidores de BD de PSFT	IP de servidor
	Objetos de PeopleSoft	Objetos
Siebel	Servidores de aplicaciones SIEBEL	IP de cliente
	Servidores de BD SIEBEL	IP de servidor
SAP	Servidores de aplicaciones SAP	IP de cliente
	Servidores de BD SAP	IP de servidor
	SAP - PCI	Objetos

Regenerar portlets de informes de aplicaciones especiales

Para algunos tipos de aplicación, se deben volver a generar uno o más portlets de informes especiales. Por ejemplo, hay dos informes EBS predefinidos y dos informes PeopleSoft predefinidos. Estos informes no se pueden modificar. Después de rellenar los grupos de aplicaciones predefinidos, siga el procedimiento para volver a generar los portlets de aplicación predefinidos y póngalos en una página.

Los ejemplos de esta sección son para los portlets de EBS, pero el procedimiento es idéntico para otros tipos de aplicación.

1. Realice una de las acciones siguientes para abrir el Buscador de informes: Usuarios con el rol de administración: Seleccione Herramientas - Creación de informes - Creador de informes. Los demás: Seleccione Supervisar/Auditar - Creación de informes - Creador de informes.
2. Pulse Buscar para abrir el panel Resultados de búsqueda de informe.
3. Seleccione un portlet de informe para el tipo de aplicación (Acceso a la aplicación EBS, por ejemplo, y pulse Regenerar portlet. Se le informará de que el portlet se ha regenerado
4. Repita el paso anterior para cada informe de aplicación (por ejemplo, Acceso a la base de datos de procesos de EBS o el informe Acceso a la base de datos de procesos de PSFT). Ahora añada un separador a su diseño e incluya los dos portlets regenerados en dicho separador.
5. Pulse Personalizar para abrir el panel Personalizar.
6. Pulse Añadir panel para definir un nuevo separador.
7. Especifique un nombre para el separador - Informes EBS, por ejemplo - y pulse Aplicar. El nuevo separador aparecerá como el último separador de la lista.
8. Pulse en el nuevo nombre de separador para editar dicho panel.
9. Pulse Añadir portlet y pulse Siguiente hasta que localice los informes que desee (por ejemplo, los informes EBS) y marque el recuadro de selección situado junto a cada informe deseado.
10. Pulse Aplicar y, a continuación, pulse Guardar y aplicar y, a continuación, pulse Guardar para guardar el nuevo diseño de panel. El nuevo separador aparecerá al final de la primera fila de separadores.
11. Pulse el nombre de separador para abrir el separador.
12. Pulse Personalizar para establecer los parámetros de tiempo de ejecución (por ejemplo, Rango de fechas y Mostrar alias).

Poco dispuesto a proporcionar DB_USER PASSWORD para la aplicación EBS

En algunos casos, los clientes no desean utilizar el DB_USER de Oracle EBS para convertir el tráfico de EBS. En este escenario, al configurar Oracle EBS y desea convertir el tráfico con la Conversión de usuarios de aplicación, existen dos opciones para que funcione:

- Proporcione el nombre de usuario y la contraseña que utiliza EBS para comunicarse con Oracle (a menudo APPS/$passwd).
- Si el cliente no desea suministrar/entrar la contraseña para el DB_USER EBS que utiliza para acceder a Oracle, todavía es posible obtener la Conversión de usuarios de aplicación; sin embargo, el proceso es más complicado.

1. Crea/elija un inicio de sesión para Oracle que permita el acceso a la base de datos para recopilar alias/usuarios/responsabilidades. Dicho usuario necesita acceder a la tabla [APPLSYS.] FND_USER y a la vista FND_RESPONSIBILITY_VL, que combina dos tablas: APPLSYS.FND_RESPONSIBILITY y APPLSYS.FND_RESPONSIBILITY_TL.

```
(  CREATE VIEW FND_RESPONSIBILITY_VL AS SELECT /* $HEADER$ */ B.ROWID ROW_ID , B.WEB_HOST_NAME ,
B.WEB_AGENT_NAME , B.APPLICATION_ID , B.RESPONSIBILITY_ID ,
B.RESPONSIBILITY_KEY , B.LAST_UPDATE_DATE , B.LAST_UPDATED_BY ,
B.CREATION_DATE , B.CREATED_BY , B.LAST_UPDATE_LOGIN ,
B.DATA_GROUP_APPLICATION_ID , B.DATA_GROUP_ID , B.MENU_ID ,
B.START_DATE , B.END_DATE , B.GROUP_APPLICATION_ID ,
B.REQUEST_GROUP_ID , B.VERSION , T.RESPONSIBILITY_NAME ,
T.DESCRIPTION FROM FND_RESPONSIBILITY_TL T, FND_RESPONSIBILITY B
WHERE B.RESPONSIBILITY_ID = T.RESPONSIBILITY_ID
AND B.APPLICATION_ID = T.APPLICATION_ID
AND T.LANGUAGE = USERENV('LANG')  )
```

2. Ejecute las siguientes sentencias SQL directamente desde el sistema Guardium: select RESPONSIBILITY_ID, RESPONSIBILITY_NAME from FND_RESPONSIBILITY_VL order by RESPONSIBILITY_ID; y SELECT USER_ID, USER_NAME from FND_USER ORDER BY USER_ID;

   Una vez que el usuario está configurado de modo que esas dos sentencias se ejecutan correctamente, se necesitan dos entradas distintas de Conversión de usuarios de aplicación. Las dos deben tener el mismo nombre de instancia, puerto e IP de servidor (y por supuesto EBS y Oracle elegidos para el tipo de APP y el tipo de servidor de APP).

   No importa si el código de aplicación es idéntico o no. Una entrada necesita el nombre de usuario que utiliza EBS para conectarse a la base de datos (normalmente APPS), pero puede colocar una contraseña incorrecta (ficticia). La segunda entrada necesita el nombre de usuario y la contraseña que se han creado para acceder a dichas tablas.

3. Una vez que las dos se han especificado con Activo y Responsabilidad seleccionados, pulse Ejecutar una vez ahora, e inicie o reinicie EBS (suponiendo que hay un motor de inspección (S-TAP o red) examinando el tráfico). Ahora se llevará a cabo la recopilación de datos y la asignación de nombres de usuario de APPS a esos datos para el tráfico de EBS.

Privilegios de Oracle necesarios para el usuario de la aplicación Oracle EBS

Conversión:

1. Otorgue selección en las tablas siguientes al usuario de BD personalizado:

   APPLSYS.FND_USER

   APPLSYS.FND_RESPONSIBILITY

   APPLSYS.FND_RESPONSIBILITY_TL

2. Cree un sinónimo FND_USER privado en APPLSYS.FND_USER para el Usuario de BD personalizado.
3. Cree una vista denominada FND_RESPONSIBILITY_VL para el usuario de BD personalizado. Puede encontrar esta vista bajo el usuario de APPS para utilizarla como plantilla.

Cómo validar la pila SAP para la Conversión de usuarios de aplicación

Cuando se da soporte a la Conversión de usuarios de aplicación de SAP de IBM Guardium, existe una diferencia entre la pila ABAP y la pila Java™.
Nota:

La pila ABAP y la pila Java tienen distintas especificaciones de kernel.

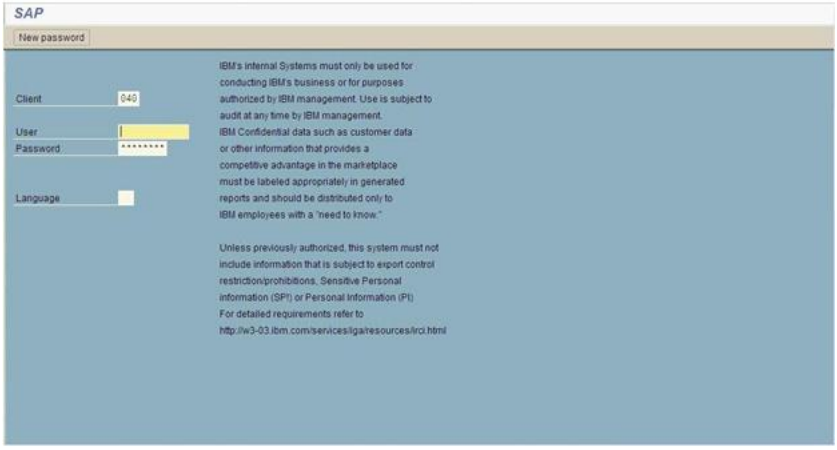
Los sistemas de pila ABAP y pila Java tendrán distintas tablas.

Pila ABAP

Los sistemas SAP tradicionales ECC (Enterprise Core Components) están escritos en código ABAP y se accede principalmente a los mismos mediante la GUI de SAP, aunque es posible el acceso web.

Los sistemas SAP ABAP tienen acceso directo (lectura/grabación/actualización) a las bases de datos SAP tradicionales. Las bases de datos son muy grandes y contienen todos los datos confidenciales. Aquí es donde IBM Guardium se utilizará mejor.

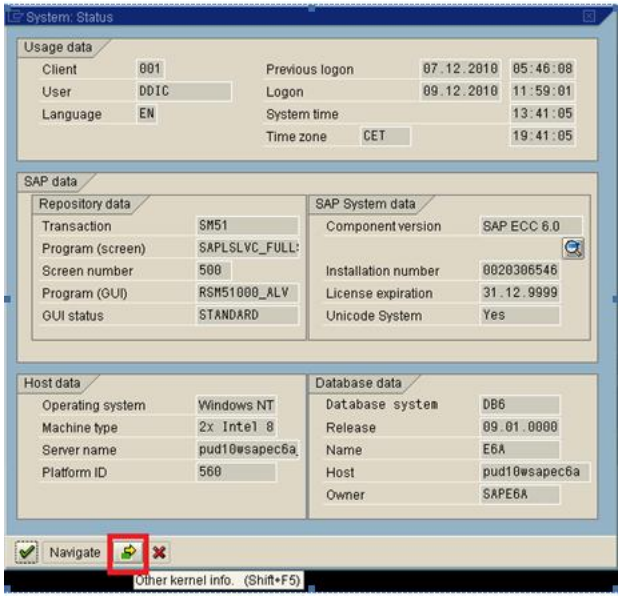
La siguiente pantalla aparecerá al entrar en la GUI de SAP (pila ABAP):



1 - GUI de SAP (pila ABAP)

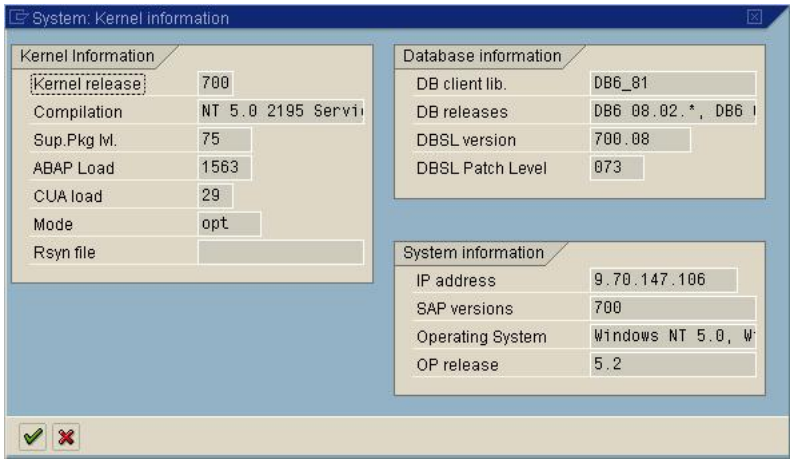
Para validar el módulo Kernel SAP de pila ABAP para la conversión de usuarios de aplicación, siga estos pasos:

1. Inicie la sesión en SAP.
2. Vaya a Sistema > Estado



2 - Estado del sistema (pila ABAP)

3. Pulse Otra información de kernel en la pantalla Estado del sistema.



3 - Información de kernel del sistema (pila ABAP)

En este ejemplo, el kernel es 700.

SAP con un programa de fondo DB2 también está disponible para el kernel SAP 640, pero el usuario necesita establecer DB6_DBSL_ACCOUNTING=1 (en el kernel 700 y más arriba, este valor DB6_DBSL_ACCOUNTING es 1 de forma predeterminada). SAP para el programa de fondo de Oracle requiere un kernel de 710 o superior.

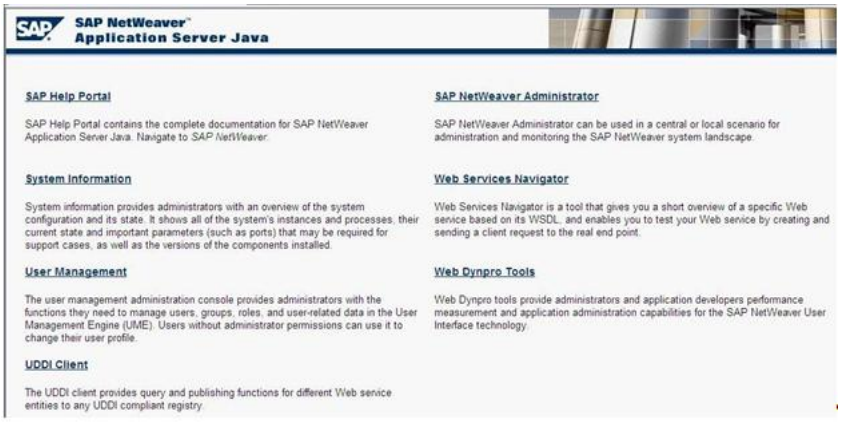
Los datos se colocan en el campo de usuario de aplicación y la serie de suceso de aplicación.

Pila Java

Los sistemas de portal SAP se escriben en código Java y son las aplicaciones web frontales que utilizan consultas predefinidas para visualizar páginas web relacionadas con SAP.

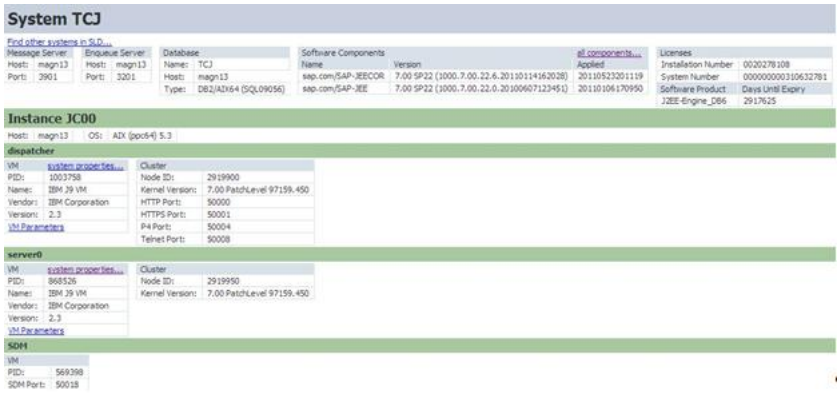
Solo se puede acceder a los sistemas de portal mediante un navegador web. Las bases de datos de sistema de portal son mucho más pequeñas con solo unos pocos espacios de tablas.

La siguiente pantalla aparecerá al entrar en el sistema de portal SAP (pila Java).



4 - Sistema de portal de SAP (pila Java)

Para validar el módulo Kernel SAP de pila Java para la conversión de usuarios de aplicación, siga estos pasos: 1. Pulse Información del sistema.



5 - TCJ del sistema (pila Java)

En este ejemplo, la versión de kernel SAP es 7.00.

SAP para DB2 u Oracle requiere un kernel de 7.02 o superior.

SAP establece propiedades de cliente similares en la pila Java tal como lo ha hecho para la pila ABAP.

Tema principal: Identificación de usuario

Identificar usuarios mediante API

Para algunas aplicaciones que gestionan usuarios internamente, el usuario de la aplicación no se puede identificar desde el tráfico. Cuando esto sucede, puede utilizar la API de sucesos de aplicación de Guardium.

La API de sucesos de aplicación proporciona llamadas sencillas que se pueden emitir desde dentro de la aplicación para indicar a Guardium cuando un usuario adquiere o libera una conexión, o cuando se produce cualquier otro suceso de interés.

Nota: Si la política de seguridad de Guardium tiene habilitado el Seguimiento de auditoría selectivo, los mandatos de la API de sucesos de aplicación que se utilizan para establecer y borrar los sucesos de usuario y/o aplicación se ignorarán de forma predeterminada y los nombres de usuario de aplicación y/o sucesos de aplicación no se registrarán. Para registrar estos elementos de modo que estén disponibles para informes o excepciones, incluya una regla de política para identificar los mandatos adecuados, especificando la acción de regla Solo auditoría.

GuardAppUser - Identificar usuarios mediante API

Utilice dos desencadenantes predefinidos para establecer GDM_CONSTRUCT_INSTANCE.APP_USER_NAME y GDM_APP_EVENT.* para los nombres de usuario de aplicación y los datos de suceso de aplicación.

Estos desencadenantes predefinidos son:

- GuardAppEvent
- GuardAppUser

Cada uno de ellos tiene desencadenantes de inicio y detención, y el suceso tiene subdesencadenantes para establecer Type, Username, StrValue, NumValue y Date.

El sistema Guardium es capaz de leer sentencias Select especiales para los detalles de AppUserName y AppEvent.

El formato es:

```
Select "action" [additional parameters] FROM [location].
```

Tabla 1. Opciones de acción

Sintaxis	Acción
GuardAppUser:<username>	Establecer GDM_CONSTRUCT_INSTANCE.APP_USER_NAME en <username>
GuardAppUserReleased	Deseleccionar APP_USER_NAME para consultas posteriores
GuardAppEvent:Start	Iniciar GuardAppEvent (y busca parámetros adicionales)
GuardAppEvent:Released	Finalizar un GuardAppEvent (borra la información de consultas subsiguientes)

Tabla 2. Parámetros adicionales (que establece los valores en GDM_APP_EVENT)

Parámetros	Sintaxis
GuardAppEventType: <event type string>	Set APP_EVENT_TYPE to <event type string>
GuardAppEventUserName:<evntursname>	Set GDM_APP_EVENT.APP_USER_NAME to <evntursname>
GuardAppEventStrValue:<strvalue>	Set EVENT_VALUE_STR to <strvalue>
GuardAppEventNumValue:<num>	Set EVENT_VALUE_NUM to <num>
GuardAppEventDateValue:<date>	Set EVENT_DATE to <date>

A continuación se muestran algunos ejemplos de sentencias select:

Select guardappuser:tiberius from dual

Select guardappuserreleased from dual

Select GuardAppEvent:Start, GuardAppEventType:Event1, GuardAppEventUserName:Tiberius, GuardAppEventStrValue:abc, GuardAppEventNumValue:123, GuardAppEventDateValue:2016-01-26 15:55:28 from dual

Select GuardAppEvent:Released from dual

La parte FROM de la sentencia varía según el tipo de base de datos.

Oracle: from DUAL

DB2 from SYSIBM.SYSDUMMY1

Informix from SYSTABLES

MS-SQL <blank>

Sybase <blank>

MySQL <blank> o from DUAL

Plantillas con nombre y nombre de usuario de aplicación de identificación de Guardium

Hay varias formas de capturar el Nombre de usuario de aplicación a través de Guardium. Guardium tiene dos tablas Turbine donde se almacenan los valores de campos APP_USER_NAME, basándose en la forma en que se reciben los datos:

GDM_CONSTRUCT_INSTANCE

GDM_APP_EVENT

El parámetro %% AppUserName de plantilla con nombre en Guardium (consulte el menú Perfil global) está correlacionado con la tabla Turbine, GDM_CONSTRUCT_INSTANCE. Para poder utilizarse en la plantilla con nombre, Guardium necesita que APP_USER_NAME en la tabla GDM_CONSTRUCT_INSTANCE se rellene con el valor de usuario de la aplicación.

Cambie la sintaxis del mandato de SQL en la aplicación por lo siguiente:

SELECT 'GuardAppUser:<value>'

Esto colocará los valores en la tabla derecha y esto sustituirá el parámetro %% AppUserName en la plantilla con nombre por el valor correcto.

Ejemplo

.....

select 'GuardAppUser:Db2_User' FROM SYSIBM.SYSDUMMY1 ;

select * from AppUser_DB2;

select 'GuardAppUserReleased' FROM SYSIBM.SYSDUMMY1 ;

select * from NoMoreUser_DB2;

.....

Busque los resultados en el archivo /var/log/messages:

Jan 24 12:49:41 vx64 guard_sender[28274]: LEEF:1.0|IBM|Guardium|10.0|Alert per match|ruleID=20003|ruleDesc=Alert per match|severity=INFO|devTime=2016-01-24
11:50:39|serverType=DB2|classification=|category=|dbProtocolVersion=3.0|usrName=Db2_User|sourceProgram=DB2JCC_APPLICATION|start=1448383760000|dbUser=DB2INST1|dst=9.70.144.126|dstPort=50000|src=9.70.144.126|srcPort=58781|protocol=TCP|type=SQL_LANG|violationID=20|sql=select * from AppUser_DB2 FOR READ ONLY|error=

Establezca el usuario de aplicación mediante GuardAppUser

Utilice esta llamada para indicar que un nuevo usuario de la aplicación ha tomado el control de la conexión. El nombre de usuario de aplicación proporcionado estará disponible en el atributo Usuario de aplicación de la entidad Período de acceso. Para esta sesión, a partir de este momento, Guardium atribuirá toda la actividad en la conexión a este usuario de aplicación, hasta que Guardium reciba otra llamada GuardAppUser o una llamada GuardAppUserReleased, que borra el nombre de usuario de la aplicación.

Para indicar cuando se producen otros sucesos (puede definir tipos de sucesos según sea necesario), utilice la llamada GuardAppEvent, que se describe en la sección siguiente.

Sintaxis: SELECT 'GuardAppUser:user_name' FROM location

user_name es una serie que contiene el nombre de usuario de aplicación. Esta serie estará disponible como el valor de atributo de Usuario de aplicación en la entidad Periodo de acceso.

FROM location solo se utiliza para Oracle, DB2 o Informix. (Se omite para otros tipos de bases de datos). Debe especificarse exactamente como se indica a continuación:

- Oracle: FROM DUAL
- DB2: FROM SYSIBM.SYSDUMMY1
- Informix: FROM SYSTABLES

Borre el usuario de aplicación mediante GuardAppUserReleased

Utilice la llamada GuardAppUserReleased para indicar que el usuario actual ha cedido el control de la conexión. Guardium borrará el nombre de usuario de la aplicación, que permanecerá vacío para la conexión hasta que reciba otra llamada GuardAppUser.

Sintaxis: SELECT 'GuardAppUserReleased' FROM location

FROM location solo se utiliza para Oracle, DB2 o Informix. (Se omite para otros tipos de bases de datos). Debe especificarse exactamente como se indica a continuación:

- Oracle: FROM DUAL
- DB2: FROM SYSIBM.SYSDUMMY1
- Informix: FROM SYSTABLES

Establecer un suceso de aplicación mediante GuardAppEvent

Esta llamada proporciona un método más genérico de señalización de la aparición de sucesos de aplicación. Puede definir sus propios tipos de suceso y proporcionar valores de texto, numéricos o de fecha para que se almacenen con el suceso, tanto cuando se inicia el suceso como cuando éste finaliza. Puede utilizar esta llamada junto con la llamada GuardAppUser. Guardium atribuirá toda la actividad de la conexión a este suceso de aplicación, hasta que reciba otro mandato GuardAppEvent:Start o un mandato GuardAppEvent:Released.

Sintaxis:

SELECT 'GuardAppEvent:Start|Released',

'GuardAppEventType:type',

'GuardAppEventUserName:name',

'GuardAppEventStrValue:string',

'GuardAppEventNumValue:number',

'GuardAppEventDateValue:date' FROM location

Start | Released: Utilice la palabra clave Start para indicar que el suceso toma el control de la conexión o Released para indicar que el suceso ha cedido el control de la conexión.

type identifica el tipo de suceso. Puede ser cualquier valor de serie, por ejemplo: inicio de sesión, cierre de sesión, crédito, débito, etc. En la entidad Sucesos de aplicación, este valor se almacena en el atributo Tipo de suceso para una llamada de inicio, o el atributo Tipo de liberación de suceso para una llamada Released.

name es un valor de nombre de usuario que se debe establecer para este suceso. En la entidad Sucesos de aplicación, este valor se almacena en el atributo Nombre de usuario de suceso para una llamada de inicio, o el atributo Nombre de usuario de liberación de suceso para una llamada de liberación.

string es un valor de serie que se debe establecer para este suceso. Por ejemplo, para un suceso de inicio de sesión puede proporcionar un nombre de cuenta. En la entidad Sucesos de aplicación, este valor se almacena en el atributo serie de valor de suceso para una llamada de inicio, o el atributo de serie de valor de liberación de suceso para una llamada de liberación.

number es un valor numérico que se debe establecer para este suceso. Por ejemplo, para un suceso de Crédito, puede proporcionar el importe de la transacción. En la entidad Sucesos de aplicación, este valor se almacena en el atributo Número de valor de suceso para una llamada de inicio o el atributo Número de valor de liberación de suceso para una llamada de liberación.

date es una fecha proporcionada por el usuario y una hora opcional para este suceso. Debe estar en el formato: aaaa-mm-dd hh:mm:ss, donde la parte de hora (hh:mm:ss) es opcional. Puede ser la fecha y la hora actuales, o puede que se tome de una transacción de la que se realiza el seguimiento. En la entidad Sucesos de aplicación, este valor se almacena en el atributo Fecha de suceso para una llamada de inicio, o en el atributo Fecha de liberación del suceso para una llamada de liberación.

FROM location solo se utiliza para Oracle, DB2 o Informix. (Se omite para otros tipos de bases de datos). Consulte el ejemplo siguiente. No obstante, cualquier nombre de tabla ficticio es aceptable para el SQL ficticio.

- Oracle: FROM DUAL
- DB2: FROM SYSIBM.SYSDUMMY1
- Informix: FROM SYSTABLES

La llamada GuardAppEvent rellena una entidad de Sucesos de aplicación (consulte Entidad de sucesos de aplicación en la sección Entidades y atributos de los Apéndices). Al crear consultas e informes de Guardium, puede acceder a la entidad Sucesos de aplicación desde el dominio de seguimiento de acceso o desde el dominio de infracciones de política.

Si algunos atributos de entidad de Sucesos de aplicación no se han establecido utilizando la llamada GuardAppEvent, esos valores estarán vacíos.

Con relación a los dos atributos de fecha:

- La fecha de suceso se establece utilizando la llamada GuardAppEvent, o desde un procedimiento de identificación personalizado, tal como se describe en la sección siguiente.
- La indicación de fecha y hora es la hora en la que Guardium almacena la instancia de la entidad Suceso de aplicación.

Tema principal: Identificación de usuario

Identificar usuarios a través de procedimientos almacenados

En muchas aplicaciones existentes, toda la información necesaria para identificar un usuario de la aplicación puede obtenerse del tráfico de la base de datos existente, a partir de las llamadas de procedimientos almacenados. Una vez que Guardium sabe qué llamadas hay que vigilar y qué parámetros contienen el nombre de usuario u otra información de interés, los usuarios se pueden identificar automáticamente.

En el caso más simple, una aplicación puede tener un solo procedimiento almacenado que establece una serie de valores, uno de los cuales es el nombre de usuario. Una llamada para establecer el nombre de usuario puede ser similar a la siguiente:

```
set_application_property('user_name', 'JohnDoe');
```

En una correlación de procedimientos personalizados (descrita más adelante), puede indicar a Guardium que:

- Observe si hay un procedimiento almacenado denominado set_application_property, con un valor de primer parámetro de user_name.
- Establezca el usuario de aplicación en el valor del segundo parámetro en la llamada (JohnDoe, en el ejemplo).

Puede haber varios procedimientos almacenados para una aplicación: uno para iniciar una sesión de usuario de aplicación, uno para finalizar una sesión y otros para iniciar una sesión y otros para indicar sucesos clave particulares para dicha aplicación. El mecanismo de procedimiento de identificación personalizado de Guardium se puede utilizar para realizar un seguimiento de los sucesos de aplicación que desee supervisar.

Puesto que cada una de las aplicaciones puede tener un modo distinto de identificar usuarios, es posible que tenga que definir correlaciones de procedimientos de identificación personalizados por separado para cada aplicación. Para hacerlo, siga el procedimiento descrito.

Definir una correlación de procedimientos de identificación personalizados

1. Vaya a Proteger > Detección de intrusión en base de datos > Procedimientos de ID personalizados.
2. Para ver una correlación existente, mantenga pulsado el puntero del ratón sobre el icono de la columna Más información para la fila que contiene la correlación que desea ver.
3. Para añadir una correlación, pulse Añadir.
4. En el recuadro Nombre de correlación personalizada, especifique el nombre que se va a utilizar para esta correlación.
5. En el recuadro Nombre de procedimiento, entre el nombre del procedimiento de base de datos que proporcionará información.
6. Seleccione Establecer o Borrar en la lista Acción para indicar si la llamada al procedimiento establecerá o borrará los valores de la aplicación. El campo Posición de tipo de suceso tiene un uso especial cuando se selecciona la acción Borrar.
7. Si la información de aplicación puede obtenerse de una llamada de procedimiento almacenado, pero solo bajo una o dos condiciones:
   - Utilice el recuadro Ubicación de condición para especificar qué parámetro de llamada de procedimiento almacenado se va a probar
   - Utilice el recuadro Valor de condición correspondiente para especificar el valor con el que debe compararse para establecer la información de la aplicación a partir de uno o varios de los otros parámetros.
   - Por ejemplo, supongamos que una aplicación utiliza un procedimiento almacenado denominado set_context para establecer un número de valores, uno de los cuales es el nombre de usuario. Al procedimiento se le pasan tres parámetros: un nombre de aplicación, un nombre de propiedad y un valor. Se ilustran tres llamadas típicas:
     - set_context('publishing_application', 'role_name', 'manager');
     - set_context('publishing_application', 'user_name', 'jsmith');
     - set_context('publishing_application', 'company', 'guardium');
   - En los ejemplos, la segunda sentencia ilustra el formato de la llamada en la que estamos interesados. El segundo parámetro (el nombre de la propiedad) es el parámetro que debe probarse, por lo que se especificaría 2 en el recuadro Ubicación de condición1 y user_name en el recuadro Valor de condición1.
   - Si un segundo formato de la llamada también establece el nombre de usuario, entonces se pueden utilizar los recuadros Ubicación y Valor de condición2. Por ejemplo, suponga que el formato siguiente de la llamada de procedimiento se utiliza a veces para establecer un nombre de usuario:
     - set_context('admin_application', 'admin_name', 'wjones');
   - Para utilizar este procedimiento, para establecer el nombre de usuario de aplicación, escriba 2 en el recuadro Ubicación de condición2 y admin_name en el recuadro Valor de condición2.
     Nota: Si se utilizan dos condiciones, el nombre de usuario o cualquier otra información que se esté extrayendo debe estar en la misma posición de parámetro para ambos tipos de llamadas.
8. Para una acción Borrar:
   - Utilice solo los campos Posición de tipo de suceso y Posición de nombre de usuario de aplicación.
   - Realice una de las siguientes acciones:
     - Para borrar el suceso de aplicación: establezca la Posición de tipo de suceso en 1 y establezca la Posición de nombre de usuario de aplicación en 0.
     - Para borrar el usuario de la aplicación: establezca la Posición de tipo de suceso en 0 y establezca la Posición de nombre de usuario de aplicación en 1.
9. Para una acción Establecer, utilice el panel Posición de parámetro para indicar qué parámetros de procedimiento almacenado se correlacionan con qué atributos de suceso de aplicación de Guardium. El primer parámetro de procedimiento tiene el número 1. Utilice 0 (cero, el valor predeterminado) para todos los atributos no establecidos por la llamada. Posición de nombre de usuario de aplicación: Escriba la posición del parámetro del nombre de usuario de aplicación que desea que esté asociado con la actividad de base de datos a partir de este punto (hasta que se restablezca, tal como se ha descrito anteriormente). Posición de valor de serie de suceso: especifique la posición de parámetro de una valor de serie para el suceso (para un inicio de sesión, esto podría ser un usuario o un nombre de cuenta). Posición de valor de número de suceso: especifique la posición de parámetro de un valor numérico para el suceso (para una transacción, esto podría ser un importe en dólares). Posición de tipo de suceso: Especifique la posición de parámetro de un nombre para el tipo de suceso (Inicio de sesión, Cierre de sesión, Solicitud de crédito, etc.) . Posición de fecha de suceso: Especifique la posición de parámetro de un valor de fecha/hora para el suceso. El formato debe ser aaaa-mm-dd hh:mm:ss. La parte de la hora (hh:mm:ss) es opcional y si se omite se establecerá en 00:00:00.

10. En el panel Información de servidor: Seleccione el tipo de servidor de base de datos en la lista Tipo de servidor. Entre el nombre de usuario de base de datos en el recuadro Nombre de usuario de BD. Opcional: Especifique un nombre de base de datos en el recuadro Nombre de base de datos. Si se omite, se supervisarán todas las bases de datos. Opcional: Identifique uno o más servidores. Si no se especifica ningún servidor, se supervisarán todos los servidores. Para seleccionar solo un servidor específico, entre la dirección IP y la máscara de red del servidor en los recuadros IP de servidor y Máscara de red de servidor; o bien, para seleccionar un grupo de servidores, seleccione un grupo de servidores en la lista Grupo de IP de servidor o pulse el botón Grupos para definir un nuevo grupo de servidores.
11. Cuando haya terminado, pulse el botón Añadir para añadir la correlación a la lista.

Tema principal: Identificación de usuario

Auditoría de cambio de valores

La característica Auditoría de cambio de valores realiza un seguimiento de los cambios en los valores de las tablas de base de datos.

La característica Auditoría de cambio de valores realiza un seguimiento de los cambios en los valores de las tablas de base de datos. Para cada tabla en la que se va a realizar un seguimiento de los cambios, debe seleccionar qué mandatos de cambio de valores SQL se deben supervisar (insertar, actualizar, suprimir). Cada vez que un mandato de cambio de valores se ejecuta en una tabla supervisada, antes y después de que se capturen los valores. De forma planificada, la actividad de cambio se sube a un sistema Guardium, donde se pueden utilizar todas las funciones de informe y generación de alertas. Los pasos básicos que se deben realizar para utilizar la característica Auditoría de cambio de valores son:

1. Cree una base de datos de auditoría en el servidor de bases de datos. Esta base de datos es donde se almacenan los datos de cambio de valor hasta que se suben en el sistema Guardium. Consulte Crear una base de datos de auditoría.
2. Identifique las tablas que se deben supervisar y, para cada tabla, seleccione los mandatos de cambio de valores (insertar, suprimir, actualizar) para los que se registrarán los cambios. Para registrar los cambios, se crea un desencadenante para cada tabla que se va a supervisar, y ese desencadenante graba los datos de cambio de valores en la base de datos de auditoría. Para permitir actualizaciones en la base de datos de auditoría (mediante el desencadenante), todos los usuarios con privilegios de actualización para la tabla supervisada reciben los privilegios adecuados para la base de datos de auditoría. Esto tiene implicaciones para los usuarios a los que se les dan privilegios de actualización para esa tabla más adelante (consulte el paso 4). Para obtener instrucciones detalladas acerca de cómo definir las actividades de supervisión, consulte Definir actividades de supervisión.
3. Planifique subidas para transferir datos de cambio de valores desde el servidor de bases de datos al sistema Guardium. Consulte Planificar subidas de cambio de valores.
4. Mantenga los privilegios de acceso a la base de datos de auditoría. Después de haber creado un desencadenante, se le puede dar acceso a un nuevo usuario a la tabla en la que se basa el desencadenante. Si dicho usuario emite un mandato de cambio de valores supervisado, fallará porque ese usuario no tendrá los privilegios adecuados para actualizar la base de datos de auditoría. Consulte Mantener listas de usuarios privilegiados.
5. Supervise la actividad de cambio desde la consola de administrador, o utilice el dominio de consulta de Seguimiento de cambio de valores para crear informes personalizados en el dispositivo de Guardium. Consulte Creación de informes de cambio de valores.

Definir actividades de supervisión

Después de definir una base de datos de auditoría, utilice el Creador de auditorías de cambio de valores para identificar las tablas que se deben supervisar y para seleccionar los tipos de cambios (inserciones, actualizaciones, supresiones) que se deben registrar.

1. Abra el Creador de auditorías de cambio de valores navegando a Reforzar > Control de cambios de configuración (Aplicación CAS) > Creador de auditorías de cambio de valores.
2. Pulse Añadir origen de datos para abrir el panel Buscador de orígenes de datos.
3. Seleccione un origen de datos en el que se ha definido una base de datos de auditoría. Si aún no se ha definido una base de datos de auditoría, consulte Crear una base de datos de auditoría.
4. Pulse Añadir para cerrar el Buscador y añadir el origen de datos seleccionado al panel Auditoría de cambio de valores.
5. Si lo desea, especifique un Propietario de esquema y/o un Nombre de objeto para limitar el número de tablas que se visualizan al elegir las tablas que se deben supervisar. Puede utilizar el carácter comodín % (porcentaje). Por ejemplo, para limitar la visualización a todas las tablas que comiencen por la letra a, especifique `a%` en el recuadro Nombre de objeto.
6. Pulse Elegir tablas a supervisar para abrir el panel Definir auditoría de datos.
7. Marque el recuadro Seleccionar para cada tabla que se va a supervisar.
   Nota: No puede definir un desencadenante para una tabla que contiene uno o más tipos de datos definidos por el usuario.

   La columna Desencandenante definido indica si ya se ha definido un desencadenante para la tabla. Los recuadros de selección Inserciones de auditoría, Supresiones de auditoría y Actualizaciones de auditoría indican si el desencadenante registrará cambios para ese mandato.

   Si la columna Desencandenante definido no está marcada, al marcar el recuadro de selección Seleccionar para una tabla se marcan automáticamente los tres recuadros de selección Auditar (Inserciones de auditoría, Supresiones de auditoría y Actualizaciones de auditoría). Si no desea supervisar uno o dos mandatos, desmarque el recuadro de selección correspondiente.

8. Pulse Añadir selecciones para definir desencadenantes para las tablas seleccionadas. Se le informará de la acción realizada.
9. Pulse Aceptar para cerrar el recuadro de mensaje y volver a visualizar el panel Definir auditoría de datos. Las tablas seleccionadas permanecen seleccionadas y la columna Desencandenante definido está ahora marcada para dichas tablas. Nota: el instante en que se define un desencadenante para una tabla, está activo y registra los cambios para los mandatos seleccionados en la base de datos de auditoría. La configuración de desencadenantes se realiza totalmente en el servidor de bases de datos, que es diferente a la mayoría de las configuraciones de Guardium, que se definen en la base de datos de Guardium y, a continuación, se activan o se desactivan como una tarea separada.
10. Para definir acciones adicionales, repita estos pasos o elimine desencadenantes marcando los recuadros de selección Seleccionar adecuados y pulsando Eliminar selecciones.
11. Pulse Hecho después de completar todos los cambios.
    Nota: El botón Cancelar no restituye los cambios que haya realizado en los desencadenantes utilizando los botones Añadir o Eliminar selecciones.

Después de definir actividades de supervisión

Si ha añadido actividades de supervisión de cambio de valores a un origen de datos por primera vez, debe planificar las subidas para este origen de datos, porque la base de datos de auditoría se vaciará solo después de que los datos registrados aquí se hayan subido al sistema Guardium. Consulte la sección siguiente.

Planificar subidas de cambio de valores

1. Abra el Creador de auditorías de cambio de valores navegando a Reforzar > Control de cambios de configuración (Aplicación CAS) > Creador de auditorías de cambio de valores.

2. Seleccione el origen de datos de auditoría para el que desea planificar subidas y pulse Planificar subida para abrir el planificador de tareas de uso general. Si necesita ayuda para definir una planificación, consulte el apartado Planificación en el manual de Herramientas comunes.

Mantener listas de usuarios privilegiados.

Cuando la característica de cambio de valores añade un desencadenante para una tabla de base de datos, todos los usuarios actuales con permiso para actualizar esa tabla tienen permiso para actualizar la tabla de base de datos de auditoría. Esto es necesario porque el desencadenante actualiza la base de datos de auditoría con valores nuevos y/o antiguos. Si a un usuario nuevo se le otorga permiso de actualización para una tabla supervisada, cuando dicho usuario intenta una actualización, la actualización no está permitida porque ese usuario no tiene también permiso para actualizar la base de datos de auditoría. Cuando esto suceda, debe actualizar la lista de usuarios con privilegios de la base de datos utilizando el Creador de auditorías de cambio de valores.

Para actualizar la lista de usuarios con privilegios de la base de datos de auditoría, el ID de usuario de base de datos que se utiliza para iniciar sesión en la base de datos supervisada debe ser el creador de cualquier rol al que se hayan añadido usuarios nuevos. De lo contrario, los miembros de ese rol no estarán disponibles.

1. Abra el Creador de auditorías de cambio de valores navegando a Reforzar > Control de cambios de configuración (Aplicación CAS) > Creador de auditorías de cambio de valores.
2. Pulse Añadir origen de datos para abrir el panel Buscador de orígenes de datos, seleccione el origen de datos adecuado en la lista y pulse Añadir.
3. Pulse Actualizar usuarios privilegiados de tablas de auditoría. Los permisos para todos los usuarios que pueden ejecutar desencadenantes para actualizar las tablas de base de datos se actualizan y se le informa cuando se completa la operación.
4. Pulse Aceptar para cerrar el recuadro de mensaje.

Creación de informes de cambio de valores

Puede ver datos de cambio de valores desde el informe Valores modificados predeterminado, o puede crear informes personalizados utilizando el dominio de Seguimiento de cambios de valores. De forma predeterminada, el dominio de Seguimiento de cambios de valores está restringido a los usuarios que tienen el rol de administración.

Informe predeterminado de valores modificados

Hay un informe de valores modificados predeterminado disponible navegando a Informes > Informes operativos de Guardium en tiempo real > Valores modificados.

La entidad principal para el informe Valores modificados es la entidad Columnas cambiadas. En la mayoría de los casos, hay una fila separada del informe para cada cambio de columna que se detecte para cada acción de auditoría (Insertar, Actualizar, Suprimir). Sin embargo, para MS SQL Server y Sybase, si la tabla supervisada no tiene una clave primaria, hay dos filas por cambio, con los valores nuevos y antiguos visualizados en filas separadas.

Tema principal: Supervisar y auditar

Crear una base de datos de auditoría

Crear una base de datos de auditoría y realizar actividades de supervisión de cambios de valores.

Para crear una base de datos de auditoría y realizar actividades de supervisión de cambios de valores, debe tener una cuenta de usuario con los permisos adecuados para:

- Crear una base de datos en el servidor
- Crear una cuenta de usuario de base de datos en el servidor

Inicie sesión en cada base de datos que se vaya a supervisar. Cree tablas y desencadenantes en cada base de datos que se vaya a supervisar.

Antes de definir una base de datos de auditoría bajo Informix o Sybase

Para Informix y Sybase (excepto para Sybase IQ, que no da soporte a desencadenantes) y en función del sistema operativo para el servidor de bases de datos, debe realizar uno de los procedimientos siguientes antes de definir la base de datos de auditoría.

Configuración de Informix - Localizar o crear un nuevo espacio de base de datos

Este tema se aplica a Informix (9.4 o posterior). En Informix, le recomendamos encarecidamente que evite utilizar el espacio de base de datos raíz predeterminado, root_dbs. No puede descartar este espacio ni reducir su tamaño.

Debe utilizar cualquier otro espacio de base de datos que se haya definido, o para crear un nuevo espacio de base de datos, realice uno de los procedimientos siguientes (en función del sistema operativo).

Informix - Crear un espacio de base de datos de Informix en un servidor Windows

Este procedimiento se realiza fuera de la GUI de Guardium y se aplica a Informix versión 9.4 o posterior.

1. Verifique que el servidor de bases de datos está en línea y a la escucha.
2. Cree un archivo de cero bytes denominado guardium_dbs_dat.000 en el directorio C:\IFMXDATA\server-name (sever-name es el nombre del servidor de Informix o el nombre de servicio). Puede hacer esto guardando un archivo de texto vacío y, a continuación, cambiando el nombre del archivo, sustituyendo el sufijo de txt por 000.
3. Haga que el siguiente directorio sea el directorio de trabajo:

   C:\Archivos de programa\Informix\bin

4. Ejecute el mandato siguiente:

   ```
   C:\Archivos de programa\Informix\bin>onspaces -c -d guardium_dbs -p C:\IFMXDATA\server-name\guardium_dbs_dat.000 -o 0 -s
   150000
   ```

   Si el archivo se ha creado satisfactoriamente, verá los mensajes siguientes:

   ```
   Verificando espacio de disco físico, espere por favor...
   Espacio añadido satisfactoriamente.
   ** AVISO ** Deberá realizarse un archivado de nivel 0 de DBSpace raíz.
   ```

5. Reinicie el servidor de Informix y utilice una herramienta adecuada (por ejemplo, el cliente remoto Aqua Data Studio) para conectar y verificar que se ha creado el espacio denominado guardium_dbs. El primer intento de conexión puede fallar con un mensaje acerca de que el servidor se ejecuta en modo desactivado temporalmente. Si esto ocurre, trate de volver a conectarse al menos dos veces más y debería funcionar.
6. Para verificar que se ha creado el espacio de base de datos de guardium_dbs, utilice Aqua Data Studio y busque en Almacenamiento.

Informix - Crear un espacio de base de datos de Informix en un servidor Unix

Este procedimiento se realiza fuera de la GUI de Guardium y se aplica a Informix versión 9.4 o posterior.

1. Desde una ventana de línea de mandatos, especifique los mandatos siguientes:

```
su - informix
cd demo/server
vi guardium_dbs
```

2. Sin añadir ningún texto, guarde el archivo guardium_dbs vacío.
3. Entre los mandatos siguientes:

```
chmod 660 guardium_dbs
cd ../../bin
onspaces -c -d guardium_dbs -p /home/informix10/demo/server/guardium_dbs -o 0 -s 100000
```

Configuración de Sybase - Inicializar discos

Este tema se aplica solo para los servidores Sybase (excepto para Sybase IQ, que no da soporte a desencadenantes). En función del sistema operativo del servidor de bases de datos, lleve a cabo uno de los procedimientos siguientes para inicializar los discos.

Sybase - Inicializar discos en un servidor Sybase de Windows

1. Conéctese al servidor en el que desea crear la base de datos de auditoría de Guardium: guardium_audit.
2. Cree una carpeta llamada guardium_audit, bajo la unidad c:.
3. Conéctese a la base de datos.
4. Ejecute los siguientes mandatos:

```
use master
go
disk init name="guardium_auditdev", size=8192
go
disk init name="guardium_auditlog",
physname="c:/guardium_audit/guardium_auditlog", size=8192
go
```

Sybase - Inicializar discos en un servidor Sybase de Unix

1. Conéctese a la base de datos.
2. Ejecute las sentencias siguientes:

```
use master
go
disk init name = 'guardium_auditdev', physname
 ='/home/sybase/data/guardium_auditdev' , size = 8192
go
disk init name = 'guardium_auditlog', physname
 ='/home/sybase/data/guardium_auditlog' , size = 8192
go
```

Crear la base de datos

Para una base de datos Informix o Sybase, asegúrese de realizar las tareas preliminares antes de realizar este procedimiento.

1. Abra el Creador de bases de datos de cambio de valores navegando a Reforzar > Control de cambios de configuración (Aplicación CAS) > Creación de base de datos de auditoría de cambio de valores.
2. Pulse Añadir origen de datos para abrir el panel Buscador de orígenes de datos. Los orígenes de datos que se han definido desde la aplicación Auditoría de cambio de valores están etiquetados como Valores de supervisor. Los orígenes de datos que se han definido para otras aplicaciones tendrán distintas etiquetas (por ejemplo, Listener o DBanalyzer), y es posible que esos orígenes de datos no tengan el conjunto adecuado de permisos de acceso a la aplicación Auditoría de cambio de valores, lo que requiere que una cuenta de usuario tenga autorización de administrador de base de datos. Si no hay disponible un origen de datos adecuado, pulse el botón Nuevo para definir uno nuevo para la base de datos que se va a supervisar (consulte Orígenes de datos en el manual de herramientas comunes para obtener información detallada sobre la definición de orígenes de datos).
   Nota: Si una base de datos GUARDIUM_AUDIT ya se ha creado en este dbserver, no se puede crear otra. La base de datos o el usuario de GUARDIUM_AUDIT deben descartarse para poder crear uno nuevo.
3. Seleccione un origen de datos que utilice una cuenta de administrador y pulse Añadir para añadirlo al panel Orígenes de datos en el panel Crear base de datos de auditoría de cambio de valores.
4. Especifique un Nombre de origen de datos de auditoría. Este es el nombre que se utilizará para identificar posteriormente el origen de datos, para definir tareas de supervisión y para subir datos. No confunda este nombre con el nombre del origen de datos del panel Orígenes de datos.
5. Opcionalmente, marque el recuadro Compartir origen de datos para compartir este origen de datos con otras aplicaciones (por ejemplo, Clasificación). El valor predeterminado es no compartir el origen de datos. Este tipo de origen de datos requiere privilegios de administrador, por lo que es posible que no desee compartir este origen de datos con otras aplicaciones.
   Nota: Para compartir un origen de datos con otros usuarios, asigne roles de seguridad a ese origen de datos.
6. Para cualquier tipo de base de datos que no sea DB2, habrá campos adicionales en el panel Configuración de auditoría. Todos los campos son necesarios. En cuanto a la tabla siguiente, especifique los valores adecuados.

Tabla 1. Tabla de campos de configuración de auditoría adicionales

Tipo de base de datos	Campo: Descripción

Tipo de base de datos	Campo: Descripción
Informix	**Espacio de base de datos**: Especifique el nombre de un espacio de base de datos existente que se va a utilizar, o especifique el nombre del espacio de base de datos que ha creado para la base de datos de auditoría (guardium_dbs en el ejemplo que se ha mostrado anteriormente). Si lo deja en blanco, se utilizará el espacio root_dbs predeterminado, lo que no es recomendable.
MS SQL Server	**Nombre de usuario de auditoría**: Especifique un nombre de usuario de base de datos nuevo para utilizarlo al acceder a la base de datos de auditoría. A este usuario se le otorgará el rol sysadmin. **Contraseña de auditoría**: Especifique una contraseña. Aparece una opción adicional en la pantalla de menú Creación de base de datos de auditoría de cambio de valores cuando el origen de datos es el servidor MSSQL. Esta opción adicional solo aparece cuando el origen de datos es el servidor MSSQL. Modalidad de compatibilidad: las opciones son Predeterminado o MSSQL 2000. Se indica al procesador la modalidad de compatibilidad que se debe utilizar al supervisar una tabla. Utilice el mandato GuardAPI, grdapi list_compatibility_modes para mostrar las modalidades de compatibilidad para MS SQL Server.
Oracle	**Contraseña de auditoría**: Especifique la contraseña para el usuario del sistema, que será la cuenta de base de datos utilizada para acceder a la base de datos de auditoría. **Espacio de tablas predeterminado**: Especifique un nombre para el espacio de tabla predeterminado. **Espacio de tabla de temporal**: Especifique un nombre para el espacio de tabla temporal.
Sybase	**Nombre de usuario de auditoría**: Especifique un nombre de usuario de base de datos nuevo para utilizarlo al acceder a la base de datos de auditoría. A este usuario se le otorgará el sa_role. **Contraseña de auditoría**: Especifique una contraseña. **Nombre de dispositivo de datos**: Especifique el mismo nombre de dispositivo de datos utilizado al inicializar el disco para la base de datos de auditoría (guardia_auditdev en el procedimiento de inicialización de disco descrito anteriormente). **Nombre de dispositivo de registro**: Especifique el mismo nombre de dispositivo de registro utilizado al inicializar el disco para la base de datos de auditoría (guardium_auditlog en el procedimiento de inicialización de disco descrito anteriormente).

7. Pulse Crear base de datos de auditoría para crear la base de datos de auditoría.
8. Utilice la selección Actualización de base de datos de auditoría de cambio de valores y Subida en el separador Configuración y control para seleccionar las acciones de esta tabla.

Acción	Descripción
Suprimir	Pulse para eliminar el origen de datos del panel Orígenes de datos.
Modificar	Pulse para editar esta definición de origen de datos en el panel Definición de origen de datos.
Planificar subida	Pulse para planificar la subida de este origen de datos de auditoría.

Después de definir la base de datos de auditoría

Una vez que se haya creado una base de datos de auditoría en un servidor de bases de datos, estará disponible para que la utilice el Creador de auditorías de cambio de valores, que es la herramienta que se utiliza para crear desencadenantes. Consulte Auditoría de cambio de valores.

Tema principal: Supervisar y auditar

Acceso a tablas supervisadas

Esta característica añade un campo “Última asesorada” a las tablas relevantes, para la interacción con productos de ciclo de vida de datos de Optim Designer.

Esta característica también se denomina “Última tabla referenciada”.

Esta característica utiliza el canal de información externo de Guardium que está preconfigurado con los datos (una correlación de canal de información externo predefinido) y un proceso de auditoría para ejecutarlo.

Siga estos pasos

1. Cree las tablas (Optim) de destino en cualquier base de datos Informix. Utilice el script.
2. Abra el Creador de procesos de auditoría navegando a Cumplir > Herramientas y vistas > Creador de procesos de auditoría y, a continuación, edite el proceso llamado Última tabla referenciada. Añada un origen de datos a la tarea Canal de información externo (el origen de datos Informix que contiene las tablas) y configure el parámetro de tiempo de ejecución para el grupo de servidores. Todo lo demás está predefinido y no hay necesidad de cambiarlo.
3. Ejecute (o planifique para que se ejecute periódicamente) el proceso de auditoría.

Nota: La tabla resultante mostrará solo la última ejecución. La cuenta de receptor es la cuenta de los receptores y no la cuenta de resultados de ejecución solo desde la última ejecución.

IBM Guardium puede detectar referencias externas a objetos de base de datos, de forma específica tablas. Esta capacidad, junto con Optim Designer, puede utilizase para gestionar la retirada de tablas inactivas o el archivado de determinadas políticas de retención.

Guardium recopila y mantiene una lista de tablas con la fecha de la última referencia. La lista se crea utilizando políticas en Guardium que dictan el intervalo de la última referencia y la frecuencia que se debe utilizar para actualizar el contenido de la lista. La información capturada por Guardium se conoce como la lista de "última referencia" y proporciona la información siguiente: ¿A qué tablas ya no se hace referencia? ¿Qué tendencias de acceso a tablas existen para los candidatos de retirada?

Tener la capacidad de planificar correctamente la retirada de las aplicaciones le ayudará a:

- Planificar la retirada o nuevo despliegue de hardware
- Reducir el coste de propiedad moviendo o retirando los recursos que dan soporte a las aplicaciones (por ejemplo, hardware, DBA, propietarios de aplicaciones, operaciones de TI, como por ejemplo copias de seguridad).
- Saber a qué tablas no se accede nunca o casi nunca

Esta funcionalidad de IBM Guardium se ha añadido directamente a la interfaz de usuario de Optim Designer.

La información proporcionada por Guardium para Optim consta de los siguientes atributos por entrada de tabla:

Tabla 1. Entrada de lista de acceso de tabla supervisada

Entrada de lista	Descripción
Campo	Comentario
DataSourceDesc	Descripción
IP de servidor	
Nombre de host	
Proveedor de BD	por ejemplo, Oracle, DB2
Nombre de usuario	por ejemplo, para Oracle mayormente define el esquema
Nombre de base de datos	
Esquema	
Tabla	
Fecha	Fecha de último acceso

Script para crear las tablas Informix en los productos Optim

Last_referenced_datasource

```
create table last_referenced_datasource (
   id              serial(1) not null,
   datasource_desc    varchar(100),
   server_ip         char(39),
   host_name          varchar(200),
   db_vendor         char(40),
   primary key (id) constraint last_referenced_datasource_pk
);
```

Last_referenced_table

```
create table last_referenced_table (
   id              serial(1) not null,
   datasource_id      int not null,
   user_name         char(32),
   db_name           char(128) not null,
   schema_name        char(128) not null,
   table_name        char(128) not null,
   last_reference     datetime year to second not null,
   primary key (id) constraint last_referenced_table_pk,
   foreign key (datasource_id) references last_referenced_datasource(id) constraint last_referenced_table_fk
);
```

Tema principal: Supervisar y auditar

Inicio rápido para la supervisión del cumplimiento

Después de desplegar agentes de supervisión (S-TAP), utilice la herramienta Supervisión del cumplimiento para establecer la supervisión para regulaciones y estándares de seguridad específicos.

Guardium proporciona varias plantillas de supervisión de cumplimiento: grupos, políticas de seguridad e informes correspondientes a regulaciones y estándares específicos, entre los que se incluyen los siguientes:

- Comité de Basel sobre supervisión bancaria (BASEL II)
- Reglamento General de Protección de Datos (GDPR)
- Reglamento General de Protección de Datos (GDPR) para Db2 for z/OS (GDPR para Db2 for z/OS)
- Health Insurance Portability and Accountability Act (HIPAA)

- Payment Card Industry Security Standard (PCI)
- Información de identificación personal (PII)
- Cumplimiento de Sarbanes-Oxley (SOX)

Estas plantillas de supervisión de cumplimiento de inicio rápido son especialmente útiles para las organizaciones que deben cumplir uno de los estándares o regulaciones asociados en un breve periodo de tiempo. Después de instalar las políticas de seguridad, la herramienta de supervisión de cumplimiento guía a los administradores o a los oficiales de cumplimiento por la configuración inicial y el relleno de grupos con información específica de la organización como, por ejemplo, direcciones IP de cliente e ID de usuarios privilegiados específicos. Además, la herramienta de supervisión de conformidad comprueba periódicamente el entorno de Guardium para ver si hay nuevas bases de datos que se puedan supervisar utilizando las plantillas de supervisión de cumplimiento.
Después de elegir una plantilla de supervisión de cumplimiento e indicar bases de datos donde debe aplicarse ese tipo de cumplimento, la herramienta de supervisión de cumplimiento lleva a cabo las siguientes acciones:

- Se crea una política de seguridad y se instala para el tipo de cumplimiento seleccionado. En un entorno gestionado centralmente, la política se instala en los recopiladores.
- Una planificación de instalación de política se define a las 10:30 diariamente. En un entorno gestionado de forma centralizada, la planificación de instalación de política se ejecuta en los recopiladores.
- Un grupo de IP de servidor se rellena con las direcciones IP de servidor de las bases de datos seleccionadas.
- El usuario actual se asigna al rol de tipo de cumplimiento seleccionado. Este rol habilita el acceso a los informes y aceleradores relacionados desde la navegación principal de Guardium.
- Cuando está soportado, se crea un escenario de descubrimiento de datos confidenciales.
- Si se crea un escenario de descubrimiento de datos confidenciales y al menos una de las bases de datos seleccionadas tiene definido un origen de datos, el escenario se planifica para que se ejecute una vez por semana los domingos a las 10:30. En un entorno gestionado de forma centralizada, la planificación se ejecuta en el gestor central.

En la tabla siguiente se resumen las características soportadas para cada uno de los tipos de cumplimiento disponibles:

Tabla 1. Resumen de las características soportadas por la herramienta Supervisión del cumplimiento por tipo de cumplimiento.

	Basel II	GDPR	HIPAA	PCI	PII	SOX
Política de seguridad	✓	✓	✓	✓	✓	✓
Informes	✓	✓		✓	✓	✓
Escenario de descubrimiento de datos confidenciales		✓		✓	✓	

- Requisitos previos para la supervisión de cumplimiento
  Revise los requisitos previos y las restricciones antes de configurar la supervisión de cumplimiento.
- Configurar supervisión del cumplimiento
  Aprenda a completar la configuración de supervisión de cumplimiento inicial.
- Rellenar grupos
  Aprenda a rellenar grupos para la supervisión de cumplimiento.
- Habilitar el escaneo de datos confidenciales
  Aprenda a almacenar credenciales de base de datos y a permitir el descubrimiento y la clasificación de datos confidenciales.
- Interpretación de las vistas de supervisión de cumplimiento
  Aprenda a interpretar y responder a las vistas de supervisión de cumplimiento.

Tema principal: Supervisar y auditar
Conceptos relacionados:
Políticas
Orígenes de datos
Tareas relacionadas:
Descubrir datos confidenciales
Información relacionada:
Grupos
Guardium GDPR Accelerator (vídeo)

Requisitos previos para la supervisión de cumplimiento

Revise los requisitos previos y las restricciones antes de configurar la supervisión de cumplimiento.

El inicio rápido para la herramienta de supervisión de cumplimiento utiliza plantillas para establecer rápidamente la supervisión de cumplimiento de los nuevos servidores de bases de datos en el entorno. Estas plantillas se han optimizado para su uso con despliegues de Guardium nuevos o en expansión. Garantice la configuración más fácil y la funcionalidad más completa verificando los siguientes requisitos previos antes de empezar:

- Usted es un usuario de Guardium con privilegios administrativos ejecutando Guardium V10.1.3 o más reciente configurado como un gestor central o un sistema autónomo.
- Los S-TAP están instalados y son operativos en los nuevos servidores de base de datos.
- Los servidores de bases de datos están soportados por las plantillas de supervisión de cumplimiento.
- No hay ninguna política instalada que no sea la política *Valor predeterminado - Ignorar actividad de datos para conexiones desconocidas*.
  Aviso:

  Puede instalar las políticas de seguridad de supervisión de cumplimiento junto con las políticas preexistentes si las políticas preexistentes tienen los siguientes valores de Definición de política:

  - Registro para proceso flat: inhabilitado
  - Reglas para proceso flat: inhabilitado
  - Seguimiento de auditoría selectivo: habilitado

  La instalación de políticas de seguridad de inicio rápido fallará si alguna política preexistente tiene valores en conflicto. Al trabajar con un despliegue existente, considere la posibilidad de desinstalar las políticas existentes antes de trabajar con las políticas de inicio rápido. Esta restricción no debería afectar a los nuevos despliegues de Guardium.

En los apartados siguientes se describen en detalle los requisitos previos de supervisión de cumplimiento de inicio rápido.

Desplegar agentes de supervisión

Antes de empezar a configurar la supervisión de conformidad, el agente de supervisión de Guardium (S-TAP) debe estar instalado en los servidores de bases de datos y estar configurado para comunicarse con el sistema Guardium. Consulte Desplegar agentes de supervisión para obtener información sobre cómo instalar y configurar rápidamente los agentes de supervisión de Guardium.

Para obtener información más detallada sobre los S-TAP, incluidos otros métodos de instalación, consulte Guía de administración de S-TAP.

Bases de datos soportadas

La herramienta de supervisión de cumplimiento detecta las bases de datos en el entorno de Guardium en función de los criterios siguientes:

- Tráfico activo en un sistema Guardium.
- El informe de instancias descubiertas (Descubrir > Informes > Instancias descubiertas).

El método de detección varía según el tipo de base de datos soportado, tal como se resume en la tabla siguiente.

Tabla 1. Resumen de tipos de bases de datos soportados y métodos de detección.

Base de datos	Tráfico activo	Instancias descubiertas
Db2 para Linux, UNIX y Windows	✓	
Db2 for z/OS	✓ Importante: La política *Valor predeterminado - Ignorar actividad de datos para conexiones desconocidas* no captura tráfico de bases de datos Db2 for z/OS. Antes de utilizar la herramienta de supervisión de cumplimiento con bases de datos Db2 for z/OS, primero debe instalar una política que cumpla con la definición de política y los criterios de tráfico activo descritos en este tema.	
Informix	✓	✓
Microsoft SQL Server	✓	✓
MySQL	✓	✓
Netezza	✓	
Oracle	✓	✓
PostgreSQL	✓	
Sybase	✓	✓
Teradata	✓	✓

El tráfico activo cumple los criterios siguientes:

- El tráfico utiliza uno de los protocolos siguientes:
  - Bases de datos Db2 for z/OS: BATCH, CALL, CICS, CTL, DRDA, PRIV, RRSAF, TRAN, TSO o UTIL.
  - Todas las demás bases de datos: TCP.
- El tráfico no es local (la IP del servidor no es igual a la IP de cliente).
- Los inicios de sesión no satisfactorios se ignoran.
- El tráfico no está cifrado.

El tráfico activo se comprueba para ver si hay nuevas bases de datos cada hora, 17 minutos después de la hora. Por ejemplo, el tráfico activo de una base de datos establecida a las 13:00 se detectará a las 13:17.
Las instancias descubiertas cumplen los criterios siguientes:

- Las bases de datos no especifican un rango de puertos.
- Las bases de datos no requieren un nombre de base de datos para la creación del origen de datos.

Reglas de extrusión e Inspeccionar datos devueltos

Varias políticas de supervisión de cumplimiento de inicio rápido utilizan reglas de extrusión. Las reglas de extrusión evalúan los datos devueltos por el servidor en respuesta a las solicitudes. Por ejemplo, una regla de extrusión puede comprobar si hay patrones numéricos asociados con datos confidenciales, como números de seguridad social o de tarjeta de crédito.

Las reglas de extrusión requieren que el valor Inspeccionar datos devueltos esté habilitado para todos los motores de inspección que utilicen la política. Para utilizar las reglas de extrusión incluidas con las siguientes plantillas de cumplimiento, debe permitir a los motores de inspección que inspeccionen los datos devueltos:

- GDPR
- HIPAA
- PCI
- PII (privacidad de datos)

Importante: La habilitación de Inspeccionar datos devueltos aumenta el tráfico de red con el conjunto de resultados devuelto.
Habilite Inspeccionar datos devueltos de Gestionar > Supervisión de actividad > Motores de inspección. Para obtener más información sobre el valor Inspeccionar datos devueltos, consulte Creación de políticas y Configuración de motor de inspección.

Valores de definición de política

Todas las políticas de seguridad de supervisión utilizan los valores de definición de política siguientes:

- Registro para proceso flat: inhabilitado
- Reglas para proceso flat: inhabilitado
- Seguimiento de auditoría selectivo: habilitado

Las políticas con valores de Registro para proceso flat, Reglas para proceso flat o Seguimiento de auditoría selectivo en conflicto no se pueden instalar en el mismo entorno de Guardium. Como resultado, no puede utilizar las plantillas de supervisión de cumplimiento de inicio rápido si ha instalado cualquier política que utilice valores diferentes.

Para nuevos despliegues o despliegues de Guardium sin políticas definidas por el usuario, es poco probable que se produzcan conflictos con estos valores de política. Para los despliegues existentes de Guardium, si recibe un mensaje de *políticas en conflicto* mientras utiliza la herramienta Configurar supervisión del cumplimiento, revise los valores de definición de política.

Para obtener más información sobre los seguimientos de auditoría selectivos, consulte Acciones de regla.
Excepción: Si es la única política instalada, la política *Valor predeterminado - Ignorar actividad de datos para conexiones desconocidas* se altera temporalmente mediante la instalación de políticas de supervisión de cumplimiento.
Tema principal: Inicio rápido para la supervisión del cumplimiento

Configurar supervisión del cumplimiento

Aprenda a completar la configuración de supervisión de cumplimiento inicial.

Antes de empezar

Para obtener más información sobre requisitos previos y restricciones, consulte Requisitos previos para la supervisión de cumplimiento.

Acerca de esta tarea

Utilice la herramienta de supervisión de cumplimiento para asociar bases de datos a una o más plantillas de cumplimiento. Este procedimiento instala rápidamente una política de seguridad, grupos, informes y un escenario de descubrimiento de datos confidenciales cuando reciba soporte.

Procedimiento

1. Abra la página de supervisión de cumplimiento accediendo a Configuración > Inicio rápido > Supervisión del cumplimiento.
2. Abra la herramienta de configuración de supervisión de cumplimiento pulsando el icono en el mosaico Configurar supervisión de cumplimiento.
3. En la sección Tipo de cumplimiento, utilice el menú Seleccione el tipo de cumplimiento desea habilitar para seleccionar el tipo de supervisión de base de datos que desea configurar. Por ejemplo, para habilitar la supervisión de GDPR, seleccione Reglamento General de Protección de Datos (GDPR). Pulse Siguiente para continuar.
4. En la sección Bases de datos, seleccione las bases de datos en la tabla Bases de datos disponibles y pulse el icono para añadirlas a la tabla Bases de datos seleccionadas.
   Sugerencias:
   - Utilice el recuadro de selección Excluir bases de datos supervisadas para ocultar bases de datos en las que ya se haya configurado la supervisión de cumplimiento.
   - Al utilizar el tipo de cumplimiento Reglamento General de Protección de Datos (GDPR) para Db2 for z/OS (GDPR para Db2 for z/OS), la lista de bases de datos disponibles se filtra para incluir solo bases de datos Db2 for z/OS. Asimismo, las bases de datos Db2 for z/OS no se visualizan cuando se trabaja con tipos de cumplimiento que no son de z/OS.
   - Seleccione las bases de datos de la tabla Bases de datos seleccionadas y pulse Proporcionar credenciales para almacenar las credenciales de base de datos. El almacenamiento de credenciales permite el descubrimiento y la clasificación de datos confidenciales para algunos tipos de cumplimiento. Si no se da soporte a la configuración automatizada, los orígenes de datos creados al almacenar credenciales se pueden utilizar en sus propios escenarios de descubrimiento de datos confidenciales.
   - Para disociar bases de datos de un tipo de cumplimiento, edite la configuración y elimine las bases de datos de la tabla Bases de datos seleccionadas o navegue desde el mosaico de tipo de cumplimiento hasta Ver detalles > Bases de datos y pulse el icono junto a una base de datos.
5. Cuando haya terminado de identificar las bases de datos que se deben supervisar, pulse Ejecutar configuración para instalar la política, rellenar el grupo de IP de servidor y ejecutar los informes de supervisión de cumplimiento.
6. En el diálogo ¿Desea renovar la página para mostrar nuevo contenido?, pulse Sí para renovar la página y completar la configuración.

Resultados

Después de configurar la supervisión de cumplimiento, verá un mosaico en el panel de control de supervisión de cumplimiento correspondiente a la plantilla de cumplimiento que ha configurado.

Qué hacer a continuación

Después de configurar la supervisión de cumplimiento, puede observar varios iconos en los mosaicos de supervisión de cumplimiento. Estos iconos indican que es necesaria configuración adicional. Utilice los enlaces Rellenar grupos para rellenar grupos adicionales o el enlace Credenciales de origen de datos para proporcionar credenciales de base de datos para un escenario de descubrimiento de datos confidenciales.

Importante: Un grupo de IP de servidor predeterminado se crea y se rellena automáticamente cuando la supervisión se configura utilizando la herramienta de configuración de supervisión de conformidad. No obstante, es importante definir los usuarios y las aplicaciones a los que se les permite acceder a las bases de datos rellenando varios grupos adicionales. Para obtener información sobre cómo rellenar grupos desde la página de supervisión de cumplimiento, consulte Rellenar grupos.
Tema principal: Inicio rápido para la supervisión del cumplimiento
Conceptos relacionados:
Requisitos previos para la supervisión de cumplimiento
Información relacionada:
Desplegar agentes de supervisión

Rellenar grupos

Aprenda a rellenar grupos para la supervisión de cumplimiento.

Antes de empezar

Instale una plantilla de supervisión de cumplimiento siguiendo el procedimiento descrito en Configurar supervisión del cumplimiento.

Acerca de esta tarea

Un grupo de IP de servidor predeterminado se crea y se rellena automáticamente cuando la supervisión se configura utilizando la herramienta de configuración de supervisión de conformidad. No obstante, es importante definir los usuarios y las aplicaciones a los que se les permite acceder a las bases de datos rellenando varios grupos adicionales. El siguiente procedimiento describe cómo rellenar grupos rápidamente.
Importante:

- Los grupos vacíos no se tratan como comodines y no capturarán ningún tráfico.
- Los grupos jerárquicos o anidados no están soportados.

Procedimiento

1. Utilice uno de los métodos siguientes para identificar los grupos no rellenados y abrir el diálogo Editar grupo para comenzar.
   - En la sección Supervisión habilitada de un mosaico de supervisión de cumplimiento, busque los iconos y pulse el enlace Rellenar grupo asociado.
   - Pulse el enlace Ver detalles en un mosaico de supervisión de cumplimiento para abrir el panel de detalles, seleccione el separador Resumen y pulse el icono junto a un grupo.
     Consejo: En el panel de detalles, los grupos no rellenados aparecen resaltados con un icono pequeño.

   En este punto, la vista de detalles y el diálogo Editar grupo se abrirán en la parte superior del panel de control de supervisión de cumplimiento.
2. En el diálogo Editar grupo, proporcione opcionalmente una Categoría y una Clasificación para el grupo. Los campos Tipo de aplicación, Tipo de grupo y Descripción (utilizados como el Nombre de grupo) se rellenan basándose en el grupo seleccionado en el paso anterior y no son editables.
3. En el diálogo Editar grupo, utilice uno de los métodos siguientes para empezar a rellenar el grupo seleccionado.
   - Pulse el icono para añadir un elemento a la tabla Miembro y especifique manualmente un miembro de grupo.
   - Pulse Importar > Desde CSV para importar miembros de un archivo CSV.
   - Pulse Importar > Desde grupo para importar miembros de grupo de otro grupo deGuardium del mismo tipo de grupo. Por ejemplo, puede rellenar un grupo de *usuarios autorizados* desde otro grupo que contenga una lista de usuarios, pero no de un grupo que contenga una lista de direcciones IP.
   - Pulse Importar > Desde origen de datos externo para importar miembros de grupos de un origen de datos externo. El menú Origen de datos incluirá todos los orígenes de datos marcados *compartidos* o de tipo *dominio personalizado*. Para obtener más información, consulte Importación desde orígenes de datos externos.
4. Cuando haya acabado de añadir miembros al grupo, pulse Aceptar para volver al panel de control de supervisión de cumplimiento.

Tema principal: Inicio rápido para la supervisión del cumplimiento

Habilitar el escaneo de datos confidenciales

Aprenda a almacenar credenciales de base de datos y a permitir el descubrimiento y la clasificación de datos confidenciales.

Antes de empezar

Instale una plantilla de supervisión de cumplimiento siguiendo el procedimiento descrito en Configurar supervisión del cumplimiento.

Acerca de esta tarea

El siguiente procedimiento describe cómo crear orígenes de datos almacenando credenciales de base de datos utilizando la herramienta de supervisión de cumplimiento. Almacenar credenciales y crear orígenes de datos permite a Guardium acceder a las bases de datos para el descubrimiento y la clasificación de datos confidenciales.

Procedimiento

1. Utilice uno de los métodos siguientes para identificar dónde son necesarias las credenciales de base de datos.
   - En la sección Escaneo de datos confidenciales de un mosaico de supervisión de cumplimiento, busque un icono y pulse el enlace Credenciales de origen de datos asociado. La vista de bases de datos de supervisión de cumplimiento se abrirá en una lista filtrada de bases de datos que requieren credenciales.
   - Pulse el enlace Ver bases de datos para abrir la vista de bases de datos de supervisión de cumplimiento y buscar las bases de datos que no tienen un icono en la columna Origen de datos.
2. En la vista de bases de datos de supervisión de cumplimiento, seleccione bases de datos que requieran credenciales y pulse Acciones de orígenes de datos > Proporcionar credenciales.
   Sugerencias:
   - Si selecciona varias bases de datos y pulsa Acciones de orígenes de datos > Proporcionar credenciales, las credenciales proporcionadas se guardarán para todas las bases de datos seleccionadas. Al proporcionar credenciales para varias bases de datos, asegúrese de que todas las bases de datos seleccionadas

utilicen las mismas credenciales. De lo contrario, las bases de datos que utilizan distintas credenciales fallarán la prueba de conexión.

- El almacenamiento de credenciales permite el descubrimiento y la clasificación de datos confidenciales para algunos tipos de cumplimiento. Si no se da soporte a la configuración automatizada, los orígenes de datos creados al almacenar credenciales se pueden utilizar en sus propios escenarios de descubrimiento de datos confidenciales.

3. En el diálogo Proporcionar credenciales, utilice los campos Nombre de usuario y Contraseña para proporcionar credenciales para las bases de datos seleccionadas. Pulse Aceptar para volver a la vista de bases de datos de supervisión de cumplimiento.
4. En la vista de base de datos de supervisión de cumplimiento, seleccione las bases de datos que tienen credenciales almacenadas y pulse Acciones de orígenes de datos > Probar conexión. Utilice Probar conexión para validar que las credenciales almacenadas permiten el acceso a la base de datos. Si la prueba de conexión falla, el descubrimiento y la clasificación de datos confidenciales no funcionarán.
   Importante:
   - La comprobación de conexiones puede requerir mucho tiempo. No es recomendable probar un número elevado de conexiones a la vez.
   - Si una prueba de conexión falla, vaya a Configuración > Herramientas y vistas > Definiciones de orígenes de datos, seleccione el origen de datos y valide la definición del origen de datos. Por ejemplo, podría necesitar especificar el puerto correcto para bases de datos Db2 for z/OS, nombres correctos de bases de datos PostgreSQL con mayúsculas y minúsculas o establecer otras propiedades de conexión necesarias para su entorno.
   - Si falla una prueba de conexión de Microsoft SQL Server, verifique que el servicio de Windows SQL Server Browser se ha iniciado.

Resultados

Después de habilitar el escaneo de datos confidenciales, los resultados de escaneo y los cambios realizados a la política (incluidos los cambios a grupos y a la pertenencia a grupos) pasarán a estar disponibles después de que la política se haya instalado de acuerdo a la planificación de instalación de políticas. De forma predeterminada, la herramienta de supervisión de cumplimiento de inicio rápido define una planificación de instalación de políticas que se ejecuta diariamente a las 10:30 de la mañana.
Tema principal: Inicio rápido para la supervisión del cumplimiento

Interpretación de las vistas de supervisión de cumplimiento

Aprenda a interpretar y responder a las vistas de supervisión de cumplimiento.

Interfaz de usuario

La herramienta Supervisión del cumplimiento consta de las siguientes vistas:

Vista de panel de control

Esta es la vista predeterminada y proporciona una visión general del estado actual del despliegue de cumplimiento, organizado por tipo de cumplimiento. Los mosaicos individuales reflejan el estado de configuración actual de varios componentes de supervisión de cumplimiento, facilitando la identificación rápida de los tipos de cumplimiento que requieren configuración adicional.

Vista de base de datos

La vista de base de datos proporciona una tabla que indica qué bases de datos se han configurado con cualquiera de las plantillas de supervisión de cumplimiento soportadas.

Configurar supervisión del cumplimiento

La herramienta Configurar supervisión del cumplimiento proporciona una interfaz guiada para asociar rápidamente bases de datos con plantillas de cumplimiento y ejecutar la configuración inicial. Acceda a la herramienta pulsando el icono en el mosaico Configurar supervisión de cumplimiento de la vista del panel de control o seleccionando bases de datos y pulsando el botón Configurar supervisión de cumplimiento en la vista de base de datos.

Las vistas de supervisión de cumplimiento proporcionan varias formas interrelacionadas para completar las tareas de configuración asociadas al establecimiento de la supervisión de cumplimiento. La tabla siguiente resume las tareas soportadas por las diferentes vistas.

Tabla 1. Resumen de las tareas soportadas por las vistas de supervisión de cumplimiento.

Tarea	Configurar supervisión del cumplimiento	Vista de panel de control	Vista de base de datos
Asociar tipo de cumplimiento con bases de datos	En la sección Bases de datos, seleccione las bases de datos de la tabla Bases de datos disponibles y pulse el icono para moverlas a la tabla Bases de datos seleccionadas.		
Rellenar grupos		Desde un mosaico de tipo de cumplimiento, pulse el enlace Rellenar grupo o vaya a Ver detalles > Resumen y pulse el icono junto a un grupo.	
Definir orígenes de datos para descubrir datos confidenciales	Desde la sección Bases de datos, seleccione bases de datos en la tabla Bases de datos seleccionadas y pulse el botón Proporcionar credenciales.	Desde un mosaico de tipo de cumplimiento, pulse el enlace Credenciales de origen de datos, seleccione las bases de datos y pulse Acciones de orígenes de datos > Proporcionar credenciales.	Seleccione bases de datos y pulse Acciones de orígenes de datos > Proporcionar credenciales.

Importante: Una vez que se ha configurado con una plantilla de supervisión de cumplimiento, las bases de datos que se han puesto fuera de línea seguirán apareciendo en la herramienta de supervisión de cumplimiento.

Políticas

Las plantillas de supervisión de cumplimiento de inicio rápido proporcionan políticas de seguridad diseñadas para trabajar de forma eficaz y sin ninguna modificación. Utilice estas políticas para ponerse en marcha rápidamente y ejecutar la supervisión de cumplimiento. Desde la vista de panel de control de supervisión de cumplimiento, pulse Ver detalles > Políticas para ver las políticas asociadas con un tipo de cumplimiento específico.

Cuando la supervisión de cumplimiento se configura desde un gestor central, las políticas de seguridad de inicio rápido se impulsan automáticamente a todos los recopiladores. Si se instalan otras políticas que no sean las políticas de seguridad de inicio rápido predeterminadas, las políticas de inicio rápido se instalan en último lugar.

Si desea revisar en detalle las políticas de supervisión de cumplimiento, éstas están disponibles a través del Buscador de políticas. Las políticas de supervisión de cumplimiento de inicio rápido se identifican con el convenio de denominación siguiente: Inicio rápido *tipo de cumplimiento*. Por ejemplo, la política GDPR predeterminada se denomina GDPR de inicio rápido. También es posible editar las políticas de seguridad de supervisión de cumplimiento utilizando el Creador de políticas para datos.
Restricción: Con anterioridad a Guardium V10.1.4, la modificación de reglas y grupos utilizados con políticas de seguridad de inicio rápido podían dar lugar a un estado de configuración imprecisos en la herramienta Supervisión del cumplimiento.
Si ha modificado las políticas de supervisión de cumplimiento, revierta a los valores predeterminados desde la vista de panel de control Supervisión de cumplimiento pulsando Ver detalles en el mosaico de tipo de cumplimiento deseado, seleccionando el separador Políticas y pulsando Restablecer a valor predeterminado. Antes de restaurar los valores predeterminados, los valores personalizados se retienen en una política con el convenio de denominación siguiente: Inicio rápido *tipo de cumplimiento indicación de fecha y hora* (donde *indicación de fecha y hora* indica que la fecha y hora en que se han restaurado los valores predeterminados). Por ejemplo, GDPR de inicio rápido 2017-05-01 19:17:59.
Importante: Con anterioridad a Guardium V10.1.4, podía ser necesario volver a instalar la política de seguridad de inicio rápido después de utilizar Restablecer a valor predeterminado. Para obtener más información, consulte Instalación de políticas de seguridad.

Planificación de instalación de política

De forma predeterminada, la herramienta de supervisión de cumplimiento de inicio rápido define una planificación de instalación de políticas que se ejecuta diariamente a las 10:30 de la mañana.

Cuando la supervisión de conformidad se configura desde una máquina autónoma, se define una planificación de instalación de política si no hay ninguna planificación de instalación de política preexistente (independientemente de si las planificaciones están activas o en pausa). Cuando se configura la supervisión de cumplimiento desde un gestor central, la planificación de instalación de política se configura para todos los recopiladores (independientemente de si hay planificaciones de instalación de política existentes).

Grupos

La herramienta de supervisión de cumplimiento se basa en varios grupos asociados a cada tipo de cumplimiento. Estos grupos deben rellenarse para establecer la supervisión de cumplimiento efectivo. Desde la vista de panel de control de supervisión de cumplimiento, pulse Ver detalles > Resumen para ver los grupos asociados a un tipo de cumplimiento específico.

Restricción:

- Los grupos jerárquicos o anidados no están soportados.
- Los grupos vacíos no se tratan como comodines y no capturarán ningún tráfico.
- Con anterioridad a Guardium V10.1.4, la modificación de reglas y grupos utilizados con políticas de seguridad de inicio rápido podían dar lugar a un estado de configuración imprecisos en la herramienta Supervisión del cumplimiento.

Puede observar una discrepancia entre el número de bases de datos y los miembros del grupo IP de servidor que se muestra en el separador Ver detalles > Resumen para un tipo de cumplimiento. Esta discrepancia refleja varias bases de datos que se ejecutan en un único grupo de servidores de bases de datos o un grupo de IP de servidor que se ha actualizado fuera de la herramienta de supervisión de cumplimiento.

Informes

Las plantillas de supervisión de cumplimiento de inicio rápido proporcionan varios informes predefinidos para cada tipo de cumplimiento. Desde la vista del panel de control de supervisión de cumplimiento, pulse Ver detalles > Informes para ver los informes asociados a un tipo de cumplimiento específico. Estos informes también están disponibles en la sección Aceleradores de la navegación principal de Guardium. Esta lista de informes está predefinida para cada tipo de cumplimiento y no refleja ningún informe personalizado que haya definido.

Restricción: La plantilla de supervisión de cumplimiento HIPAA no proporciona ningún informe predefinido.

Usuarios y roles

El usuario actual se asigna al rol de tipo de cumplimiento seleccionado. Este rol habilita el acceso a los informes y aceleradores relacionados desde la navegación principal de Guardium. Si diferentes usuarios de Guardium configuran distintos tipos de cumplimiento, los usuarios individuales solo tendrán acceso a los informes y a los aceleradores asociados con los tipos de cumplimiento que configuraron.

Por ejemplo, si *user1* configura *GDPR* y *user2* configura *PCI*, *user1* no tendrá acceso a los informes PCI ni a los aceleradores porque el rol de PCI no se ha asignado a *user1*. Para obtener información sobre cómo asignar manualmente roles específicos a los usuarios, consulte Visión general de la gestión de accesos.

Datos confidenciales

Puede observar una discrepancia entre el valor Coincidencias encontradas en un mosaico de tipo de cumplimiento y los grupos de objetos asociados en el separador Detalles de vista > Resumen. Coincidencias encontradas indica el número de pares de nombres de tabla y columna exclusivos que coinciden con los criterios del escenario de descubrimiento de datos confidenciales. El número de miembros en el grupo OBJETOS es el número de nombres de tabla exclusivos y es un valor acumulativo de todos los escaneos.

Importante: En la sección Escaneo de datos confidenciales de un mosaico, los iconos indican que se ha configurado uno o varios orígenes de datos para el escenario de descubrimiento de datos confidenciales. Pulse Ver bases de datos para investigar qué bases de datos tienen orígenes de datos definidos para el descubrimiento de datos confidenciales.
Tema principal: Inicio rápido para la supervisión del cumplimiento

Cómo utilizar PCI/DSS Accelerator para implementar el cumplimiento de PCI

Configure PCI/DSS Accelerator de IBM Security Guardium's y cree una serie de políticas e informes para cumplir con los requisitos de PCI/DSS.

PCI/DSS (Payment Card Industry/ Data Security Standard) es un conjunto de requisitos técnicos y operativos diseñados para proteger datos de titulares de tarjetas.

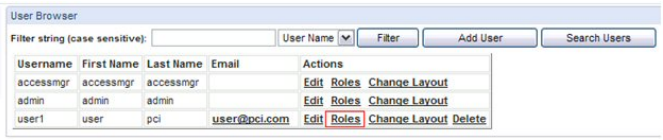
Valor añadido: Proporciona a los clientes una vista completa de PCI/DSS y proporciona políticas e informes predefinidos para ahorrar tiempo de configuración.

Siga estos pasos:

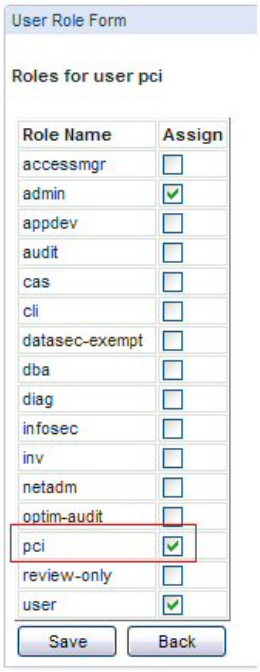
1. Configure el rol PCI.
2. Configure informes y políticas que siguen los requisitos.

Configure el rol de PCI

1. Inicie sesión a través de la página de la interfaz gráfica de usuario de Guardium utilizando la cuenta de usuario "accessmgr". Seleccione un usuario (in en este caso, user1) y pulse Roles.

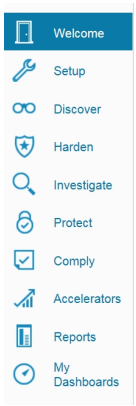


2. En el formulario de rol de usuario, seleccione PCI y, a continuación, guarde la asignación.



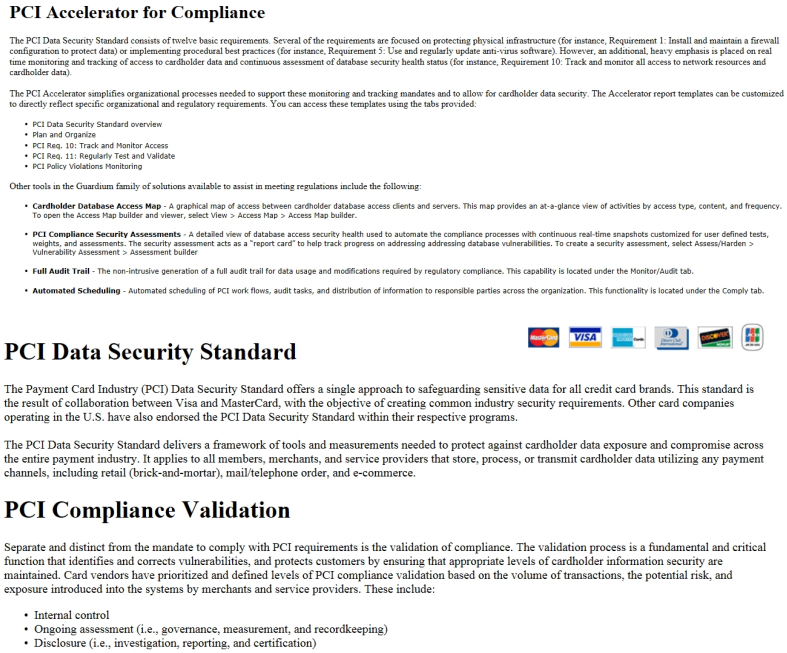
Implementar PCI Accelerator

Inicie la sesión utilizando "user1" y pulse Aceleradores.



Visión general

1. Pulse PCI Accelerator for Compliance.
2. Pulse PCI Data Security Standard.



PCI Accelerator for Compliance

The PCI Data Security Standard consists of twelve basic requirements. Several of the requirements are focused on protecting physical infrastructure (for instance, Requirement 1: Install and maintain a firewall configuration to protect data) or implementing procedural best practices (for instance, Requirement 5: Use and regularly update anti-virus software). However, an additional, heavy emphasis is placed on real time monitoring and tracking of access to cardholder data and continuous assessment of database security health status (for instance, Requirement 10: Track and monitor all access to network resources and cardholder data).

The PCI Accelerator simplifies organizational processes needed to support these monitoring and tracking mandates and to allow for cardholder data security. The Accelerator report templates can be customized to directly reflect specific organizational and regulatory requirements. You can access these templates using the tabs provided:

- PCI Data Security Standard overview
- Plan and Organize
- PCI Req. 10: Track and Monitor Access
- PCI Req. 11: Regularly Test and Validate
- PCI Policy Violations Monitoring

Other tools in the Guardium family of solutions available to assist in meeting regulations include the following:

- **Cardholder Database Access Map** - A graphical map of access between cardholder database access clients and servers. This map provides an at-a-glance view of activities by access type, content, and frequency. To open the Access Map builder and viewer, select View > Access Map > Access Map builder.
- **PCI Compliance Security Assessments** - A detailed view of database access security health used to automate the compliance processes with continuous real-time snapshots customized for user defined tests, weights, and assessments. The security assessment acts as a "report card" to help track progress on addressing addressing database vulnerabilities. To create a security assessment, select Assess/Harden > Vulnerability Assessment > Assessment builder
- **Full Audit Trail** - The non-intrusive generation of a full audit trail for data usage and modifications required by regulatory compliance. This capability is located under the Monitor/Audit tab.
- **Automated Scheduling** - Automated scheduling of PCI work flows, audit tasks, and distribution of information to responsible parties across the organization. This functionality is located under the Comply tab.

PCI Data Security Standard

The Payment Card Industry (PCI) Data Security Standard offers a single approach to safeguarding sensitive data for all credit card brands. This standard is the result of collaboration between Visa and MasterCard, with the objective of creating common industry security requirements. Other card companies operating in the U.S. have also endorsed the PCI Data Security Standard within their respective programs.

The PCI Data Security Standard delivers a framework of tools and measurements needed to protect against cardholder data exposure and compromise across the entire payment industry. It applies to all members, merchants, and service providers that store, process, or transmit cardholder data utilizing any payment channels, including retail (brick-and-mortar), mail/telephone order, and e-commerce.

PCI Compliance Validation

Separate and distinct from the mandate to comply with PCI requirements is the validation of compliance. The validation process is a fundamental and critical function that identifies and corrects vulnerabilities, and protects customers by ensuring that appropriate levels of cardholder information security are maintained. Card vendors have prioritized and defined levels of PCI compliance validation based on the volume of transactions, the potential risk, and exposure introduced into the systems by merchants and service providers. These include:

- Internal control
- Ongoing assessment (i.e., governance, measurement, and recordkeeping)
- Disclosure (i.e., investigation, reporting, and certification)

Planificar y organizar

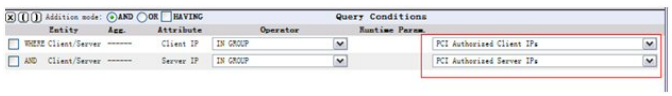
Planificar y organizar

Pulse la Visión general para obtener una introducción de cómo los informes predefinidos siguen el cumplimiento.

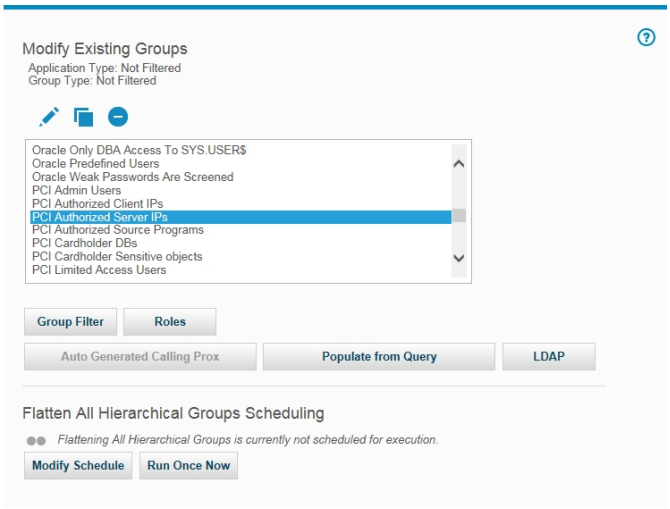
1. Lista de IP del servidor de titulares de tarjeta: Lista de servidores de base de datos de información de titulares de tarjetas. Según la situación real de la empresa, establezca la información de grupo de IP de servidores autorizados por PCI, que especifica el servidor de bases de datos que almacena la información de titulares de tarjetas.
2. Bases de datos de titulares de tarjetas: Base de datos de información de titulares de tarjetas. Establecer la base de datos de titulares de tarjetas de PCI: información de grupo designada, que se almacena en la información de titulares de tarjetas en la base de datos.
3. Objetos de titulares de tarjetas: Objeto de información de titulares de tarjetas. Esto necesita establecer los objetos confidenciales de titulares de tarjetas de PCI.
4. Correlación de clientes de base de datos con servidores: La correlación de cliente/servidor y la información de grupo de conjunto de IP de servidores autorizados por PCI, que especifica los servidores de base de datos que almacenan información de titulares de tarjetas. La consulta se puede utilizar para buscar acceso de cliente a la base de datos de titulares de tarjetas.
5. Usuarios de base de datos activos: Administrador además de categorías de usuarios, que han visitado la base de datos de titulares de tarjetas. Establezca las “IP de servidores autorizados por PCI” y “Usuarios administradores de PCI”.
6. Administración de base de datos de titulares de tarjetas: Operaciones de gestión de base de datos de titulares de tarjetas. Establezca los usuarios administrativos y las IP de servidores autorizados por PCI.
7. Programas fuente autorizados: Acceso a programa de crédito. Establezca las IP de servidores autorizados de PCI, Programas fuente autorizados por PCI. Procedimiento para registrar el acceso a la base de datos de titulares de tarjetas de crédito.
8. Acceso a las aplicaciones no autorizado: Acceso a programa no de crédito. Establezca las IP de servidores autorizados de PCI, Programas fuente autorizados por PCI. Registros de programa de crédito para el acceso a base de datos de titulares de tarjetas.
9. 8.5.8 Cuentas compartidas: requisitos de ocho PCI para que a cada persona que tenga acceso al sistema se le asigne un ID exclusivo. Establezca las IP de servidores autorizados por PCI para contar el número de veces que el mismo nombre de usuario de base de datos intenta acceder desde la IP de base de datos de titulares de tarjetas.

En las sentencias, pulse para ver un formato de informe y, a continuación, determine qué contenido de grupo específico se debe rellenar.

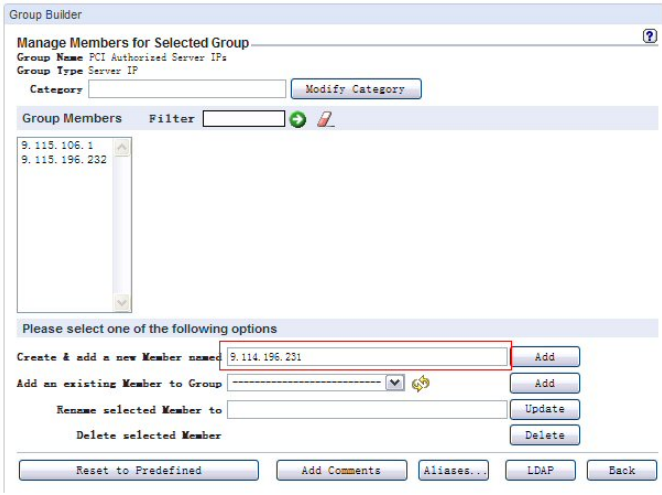
A continuación se muestra el nombre real del grupo:



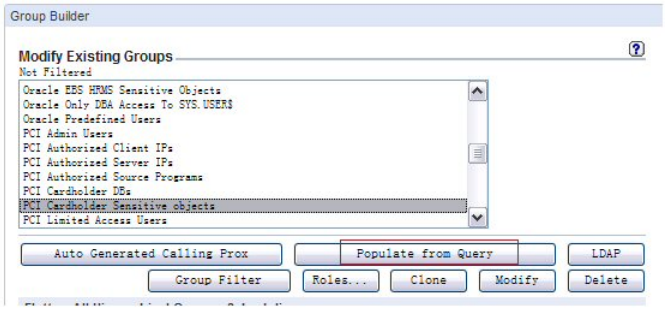
Vaya a Configuración > Herramientas y vistas > Creador de grupos y, en la selección Modificar grupos existentes, seleccione el nombre del grupo.



Pulse Modificar (el icono de lápiz) y vaya a la página Gestionar miembros del grupo seleccionado. Añada miembros nuevos.



El grupo también puede rellenarse a través de una consulta personalizada.



Requisito 10 de PCI - Realizar seguimiento y Supervisar

Pulse la Visión general para ver una introducción de cómo el supervisor de Guardium y los informes predefinidos siguen el cumplimiento.

1. Automatización de 10.2 y 10.3: Utilice el documento de ayuda Proteger de ayuda y el documento de ayuda Cumplir de la ayuda en línea para automatizar esta sección.
2. 10.2.1 Acceso a datos: Acceso de PCI a los datos del titular de la tarjeta. Establecer las IP de servidor autorizadas de PCI y los Usuarios de administración de PCI.
3. 10.2.2 Actividad de administrador: Actividad de PCI por usuario administrador. Establecer las IP de servidores autorizados por PCI y los usuarios de administración de PCI.
4. 10.2.3 Acceso de seguimiento de auditoría: Para seguir completamente esta sección, se deben definir al menos cuatro clases de informes: Inicios de sesión en SQLGuard; Seguimientos de auditoría de la actividad de usuario en el servidor de Guardium; Excepciones de trabajos planificados y listas de tareas pendientes de usuarios.Vaya a Configuración > Informes > Creador de informes para crear informes según sea necesario.
5. 10.2.4 Acceso no válido - PCI - Intentos de acceso de inicio de sesión no válidos: el registro de inicio de sesión ha fallado, intente en la base de datos. PCI - Acceso a las aplicaciones no autorizado: no se ha definido registro de acceso a base de datos en los Programas fuente autorizados de PCI.
6. Estas tres secciones también pueden utilizar el documento de ayuda Supervisar y auditar en la ayuda en línea que se incluye - 10.2.6 Registro de inicialización, 10.5 Proteger seguimientos de auditoría y 10.6 Auditoría de acceso.

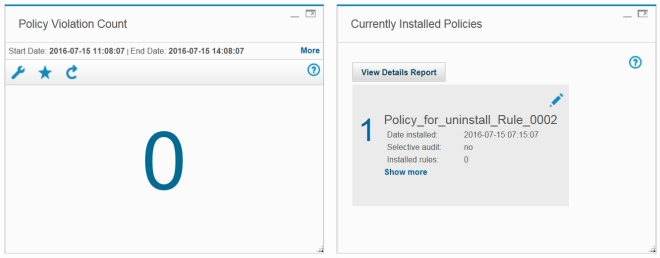
Requisito 11 de PCI - Validación en curso

Pulse Visión general para ver una discusión sobre la importancia del asesoramiento de vulnerabilidades. Pulse Reforzar > Creador de asesoramientos para crear un proceso de asesoramiento.

Supervisión de políticas de PCI

Pulse Visión general para introducir la política.

1. Para mostrar las instalaciones de política actuales, vaya a Configurar > Herramientas y vistas > Instalación de políticas y elija una política adecuada para la instalación.



2. Infracciones de política - Registros de las operaciones de infracciones.

Tema principal: Supervisar y auditar

Creador de flujos de trabajo

El Creador de flujos de trabajo se utiliza para definir flujos de trabajo personalizados (pasos, transiciones y acciones) para que se utilicen en el proceso de auditoría.

Para obtener más información, consulte Creación de procesos de auditoría. Siga estos pasos para:

- Definir los pasos de flujo de trabajo (estado de suceso),
- Definir el flujo del tránsito entre un paso y otro (acciones)
- Definir qué acciones requieren aprobación
- Asignar roles a cada estado, para definir los usuarios con permiso para ver cada estado

Términos relevantes para esta característica

Tipo de suceso: Flujo de trabajo personalizado

Estado de suceso: Estado del flujo de trabajo.

Acción de suceso: Acción/Transición

Nota: El Creador de flujos de trabajo es un componente opcional habilitado por la clave de producto.

Crear un Creador de flujos de trabajo

1. Con una cuenta de administrador, abra el Creador de flujos de trabajo navegando hasta Cumplir > Herramientas y vistas > Creador de flujos de trabajo. Con una cuenta de usuario que tenga privilegios DataPrivacy, abra el Creador de flujos de trabajo navegando a Aceleradores > Privacidad de datos > Rastrear y supervisar > Seguimiento de auditoría y Automatización del flujo de trabajo.
2. En la primera pantalla (Tipo de suceso), pulse Estado de suceso para ir a la configuración de Estado de suceso.
3. Pulse Añadir estado de suceso para definir un estado de suceso nuevo. Se esperan varios estados de suceso. Rellene la descripción de estado y ponga una marca de selección en el recuadro de selección Es final si la tarea es una tarea final en el flujo de trabajo.
4. Pulse Tipo de suceso y, a continuación, pulse Añadir en Añadir definición de tipo de suceso para definir un tipo de suceso nuevo.
5. Rellene la descripción y designe la primera tarea en el flujo de trabajo.
6. A continuación, elija el estado permitido para el flujo de trabajo en la lista de estados permitidos, resaltando el elemento Estado y pulsando en el botón > entre la lista de estados disponibles y la lista de estados permitidos.
7. Cuando haya terminado, pulse el botón Guardar. Nota: El botón Guardar (o el botón Cancelar) solo se aplica a los cambios realizados en el nombre, el suceso predeterminado o los sucesos disponibles.
8. Vaya a la sección Acciones de suceso definidas de la pantalla de menú Tipo de suceso. Las acciones de suceso definidas incluye la designación de acciones de sucesos separadas del flujo de trabajo.
9. Pulse el botón Nuevo.
10. Rellene la Descripción de acción de suceso y designe el estado anterior, el estado siguiente y si es necesaria la aprobación de esta acción de suceso. Pulse el botón Aplicar.
11. Repita los pasos 9 y 10 hasta que todas las acciones de sucesos estén descritas y designadas.
12. Vaya a la sección Roles de la pantalla de menú Tipo de suceso. Los roles implican la definición de quién puede ver el suceso cuando está en una acción de suceso determinada. Por ejemplo, quién puede ver los sucesos que están "Bajo revisión" y quién puede ver los sucesos que están "Aprobados".
13. Seleccione el Estado de tipo de suceso y pulse el botón Roles.
14. En el panel Asignar roles de seguridad, marque todos los roles que desea asignar (solo verá los roles que se han asignado a la cuenta). Pulse Aplicar para guardar las opciones de rol de seguridad. Pulse el botón Atrás.
15. Repita los pasos 13 a 14 hasta que se haya definido roles para todos los estados de tipo de suceso.
16. Se ha realizado el esfuerzo de configuración del Creador de flujos de trabajo.
17. Abra el Creador de procesos de auditoría navegando a Cumplir > Herramientas y vistas > Creador de procesos de auditoría para planificar el flujo de trabajo y crear y mostrar informes de flujo de trabajo. Consulte los pasos del Creador de procesos de auditoría bajo Definir una tarea de informe.

Hay un escenario de uso, Ejemplo de flujo de trabajo de creador de flujos de trabajo en los Apéndices .

Nota: Si el tipo de tarea en el Creador de proceso de auditoría es Proceso de clasificación, entonces el Creador de flujos de trabajo no puede crear flujos de trabajo personalizados.

Nota de aviso: Cuando se crea un suceso de flujo de trabajo, se puede asignar un rol a cada estado utilizado por dicho suceso (lo que significa que sólo se pueden ver con este rol en este estado). Cuando se asigna un suceso a un proceso de auditoría, es importante que cada rol que se asigne a un estado de este suceso tenga un receptor en este proceso de auditoría. De lo contrario, es posible que una fila de resultado de auditoría pueda colocarse en un estado en el que ninguno de sus receptores pueda ver esta fila o cambiar su estado.

Si una fila de auditoría pasa a ser inaccesible, el usuario administrador (que es capaz de ver todos los sucesos, independientemente de sus roles) podría ver la fila y cambiar su estado. Sin embargo, si la seguridad a nivel de datos está activada, es posible que el usuario administrador no pueda ver esta fila. El usuario administrativo tendría que desactivar la seguridad a nivel de datos (desde el perfil global) o tener el rol dataset_exempt. Es importante configurar el proceso de auditoría para que todos los roles que deban actuar en un suceso asociado a este proceso de auditoría sean receptores de este proceso de auditoría.

Nota: La supresión de un estado de suceso solo se permite si el estado no está en el primer o último estado de cualquiera de los sucesos y si no lo utiliza ninguna acción. La validación proporcionará una lista de sucesos/acciones que impiden que el estado se suprima.

Añadir sucesos predeterminados solo a un número de registros limitado

Al ejecutar una tarea de informe de proceso de auditoría, los resultados de esta tarea de proceso se guardan en la tabla, REPORT_RESULT_DATA_ROW. Esta tabla tendrá una fila para cada fila del informe. Si esta tarea de informe también tiene asignado un suceso predeterminado, se añade una fila a la tabla, TASK_RESULT_ADDITIONAL_INFO, para cada fila del informe. Esto puede dar lugar a un problema de espacio de disco solo si se utilizan sucesos para resultados grandes. Cree sucesos solo en los resultados de la tarea con un número limitado de registros; de lo contrario, los usuarios nunca podrán gestionar el gran número de registros. Si se utilizan sucesos predeterminados de la forma limitada prevista, no habrá problemas de espacio de disco ni ningún problema de usabilidad, ya que no es fácil cerrar miles de sucesos.

- Cómo crear flujos de trabajo personalizados
  Definir flujos de trabajo personalizados formados por pasos, transiciones y acciones específicos del cliente para que se utilicen adicionalmente en un proceso de auditoría.
- Cómo utilizar los flujos de trabajo personalizados
  Defina un proceso de auditoría que siga las prácticas de flujo de trabajo personalizadas del cliente. Lleve los procesos y las prácticas de auditoría específicos del cliente a la solución Guardium.

Tema principal: Supervisar y auditar

Cómo crear flujos de trabajo personalizados

Definir flujos de trabajo personalizados formados por pasos, transiciones y acciones específicos del cliente para que se utilicen adicionalmente en un proceso de auditoría.

Acerca de esta tarea

Definir y gestionar el flujo de trabajo basándose en prácticas específicas del cliente.

Consulte Creador de flujos de trabajo para ver una visión general de este componente.

Requisitos previos

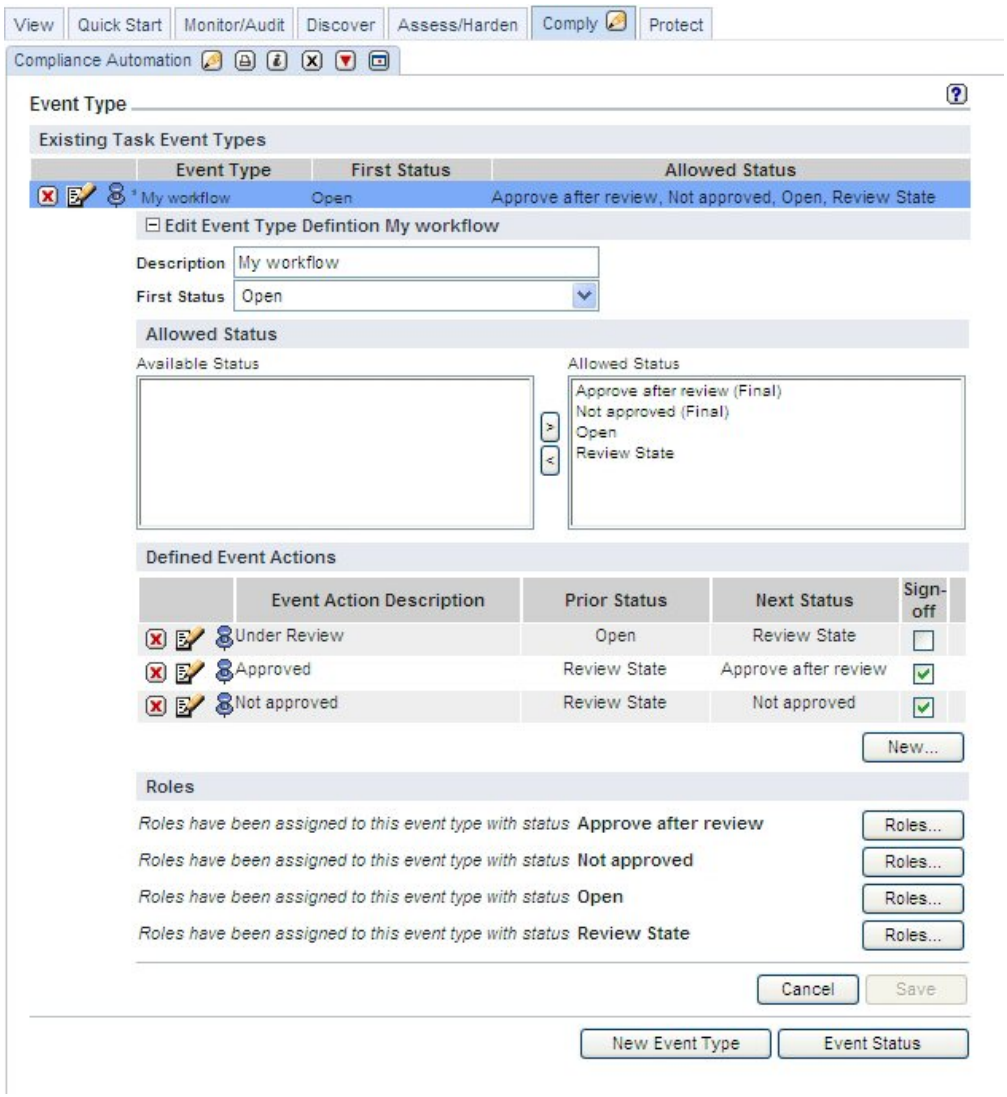
- Consulte Cómo crear un flujo de trabajo de auditoría. Para obtener información adicional, consulte la sección Automatización de flujo de trabajo de cumplimiento.
- Después de crear este flujo de trabajo personalizado, consulte Cómo combinar flujo de trabajo personalizado con flujo de trabajo de auditoría.

Procedimiento

1. Abra el Creador de flujos de trabajo navegando a Cumplir > Herramientas y vistas > Creador de flujos de trabajo.
2. En la primera pantalla (Tipo de suceso), pulse el botón Estado de suceso para ir a la configuración de Estado de suceso.
3. Pulse Añadir estado de suceso para definir un nuevo estado de suceso. Se esperan varios estados de suceso. Rellene la descripción de estado y ponga una marca de selección en el recuadro de selección Es final si la tarea es una tarea final en el flujo de trabajo. Cuando haya terminado, vaya al paso siguiente.

   Un ejemplo de un flujo de trabajo simple de tres pasos es: Abrir para Revisar estado o Aprobar o No aprobado. Cada paso del flujo de trabajo es un Estado de suceso de tarea definido separado.

   Las tareas de flujo de trabajo del ejemplo son: Abrir, Revisar estado, Aprobar después de revisar o No aprobado. Además, si la tarea es la última tarea en un flujo de trabajo, ponga una marca de selección en la columna Es final. Ejemplos de una tarea final en el ejemplo son Aprobado o No aprobado.



4. Pulse el botón Tipo de suceso y luego pulse el botón Añadir de Añadir definición de tipo de suceso para definir un nuevo Tipo de suceso.
5. Rellene la descripción y designe la primera tarea en el flujo de trabajo.
6. A continuación, elija el estado permitido para el flujo de trabajo en la lista de estados permitidos, resaltando el elemento Estado y pulsando en el botón > entre la lista de estados disponibles y la lista de estados permitidos.
7. Cuando haya terminado, pulse el botón Guardar.
8. Vaya a la sección Acciones de suceso definidas de la pantalla de menú Tipo de suceso. Las acciones de suceso definidas incluye la designación de acciones de sucesos separadas del flujo de trabajo.
9. Pulse el botón Nuevo.

   En el ejemplo de flujo de trabajo de tres pasos simple, una acción de suceso de bajo revisión tiene un estado anterior de abierto y un estado siguiente de Revisar estado. La Acción de suceso de Aprobado sigue Bajo revisión con un estado anterior de Revisar estado y el siguiente estado de Aprobar después de revisar. O, la Acción de suceso de No aprobada tiene un estado anterior de Revisar estado y un estado siguiente de No aprobado. También hay una capacidad de aprobación para los revisores designados por la acción de suceso (continua o secuencial). Consulte la captura de pantalla anterior.

10. Rellene la Descripción de acción de suceso y designe el estado anterior, el estado siguiente y si es necesaria la aprobación de esta acción de suceso. Pulse el botón Aplicar.
11. Repita los pasos 9 y 10 hasta que todas las acciones de sucesos estén descritas y designadas.
12. Vaya a la sección Roles de la pantalla de menú Tipo de suceso. Los roles implican la definición de quién puede ver el suceso cuando está en una acción de suceso determinada. Por ejemplo, quién puede ver los sucesos que están "Bajo revisión" y quién puede ver los sucesos que están "Aprobados".
13. Seleccione el Estado de tipo de suceso y pulse el botón Roles.
14. En el panel Asignar roles de seguridad, marque todos los roles que desea asignar (solo verá los roles que se han asignado a la cuenta). Pulse Aplicar para guardar las opciones de rol de seguridad. Pulse el botón Atrás.
15. Repita los pasos 13 a 14 hasta que se haya definido roles para todos los estados de tipo de suceso.
16. Se ha realizado el esfuerzo de configuración del Creador de flujos de trabajo.
17. Abra el Creador de procesos de auditoría navegando a Cumplir > Herramientas y vistas > Creador de procesos de auditoría para planificar el flujo de trabajo y crear y mostrar informes de flujo de trabajo. Consulte los pasos del Creador de procesos de auditoría bajo Definir una tarea de informe.

Tema principal: Creador de flujos de trabajo

Cómo utilizar los flujos de trabajo personalizados

Defina un proceso de auditoría que siga las prácticas de flujo de trabajo personalizadas del cliente. Lleve los procesos y las prácticas de auditoría específicos del cliente a la solución Guardium.

Acerca de esta tarea

Flujos de trabajo personalizados en el proceso de flujo de trabajo de auditoría de Guardium

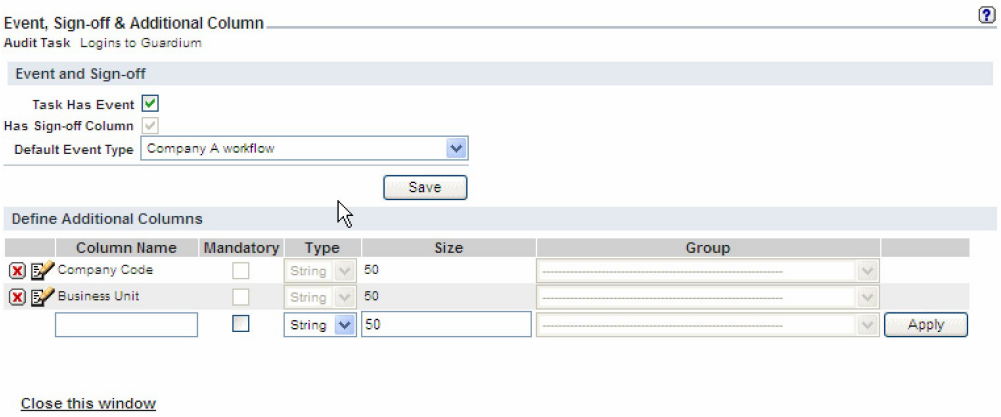
La secuencia formal de tipos de sucesos creados en el Creador de flujos de trabajo se gestiona pulsando en el botón Suceso y columnas adicionales en la ventana Tareas de auditoría. Este botón aparecerá después de que se haya creado y guardado una tarea de auditoría. Este botón adicional no aparecerá hasta que se guarde la tarea de auditoría.

Requisitos previos

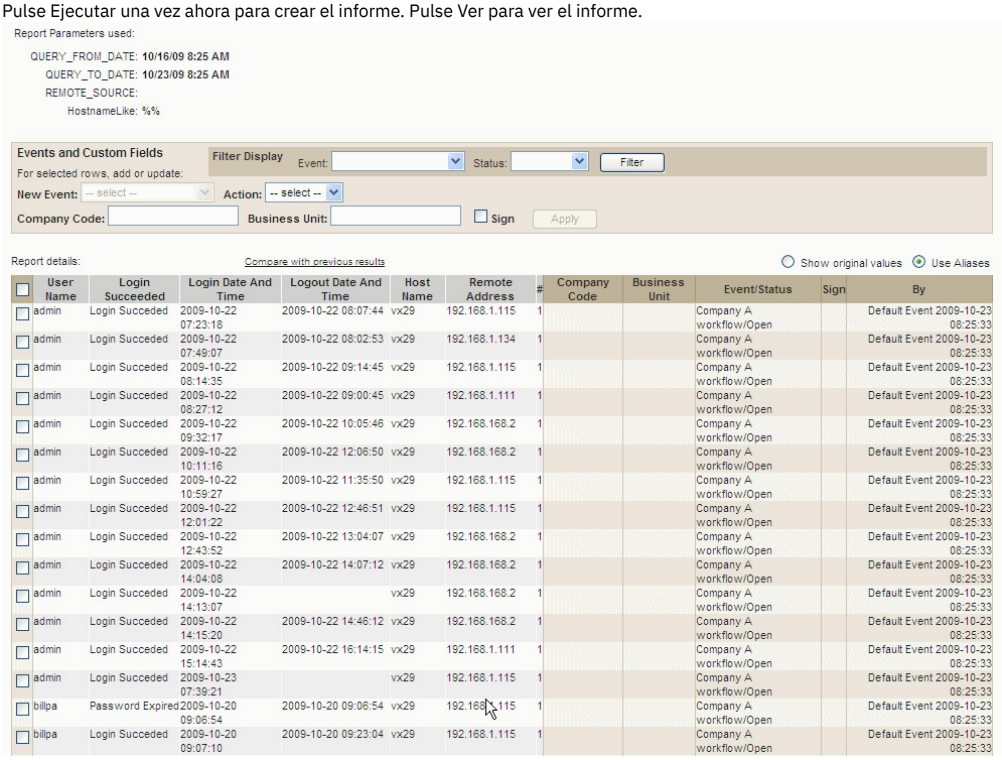
- Consulte Cómo crear flujos de trabajo personalizados. Para obtener información adicional, consulte Crear flujos de trabajo.
- Consulte Cómo crear un flujo de trabajo de auditoría. Para obtener información adicional, consulte la sección Automatización de flujo de trabajo de cumplimiento.
- Defina un proceso de auditoría que siga las prácticas de flujo de trabajo personalizadas del cliente efectuando los pasos adicionales.

Procedimiento

1. Configure estas actividades de flujo de trabajo al añadir una tarea de auditoría.
2. Cree y guarde una tarea de auditoría. Después de guardar, aparecerá un botón adicional, Sucesos y Columnas adicionales.
3. Pulse este botón adicional.



4. En la siguiente pantalla, ponga una marca de selección en el recuadro para Suceso y aprobación. El flujo de trabajo creado en Creador de flujos de trabajo aparecerá como una opción en Suceso y aprobación.
5. Resalte esta opción. Guarde la selección.
6. Si es necesaria información adicional (como códigos de empresa, etiquetas de unidades de negocio, etc.) como parte del informe de flujo de trabajo, añada esta información en la sección Columna adicional de la pantalla y luego pulse Aplicar (guardar). Cuando haya terminado, cierre esta ventana.
7. Aplique (guarde) su tarea de auditoría. Aplique (guarde) toda la definición del proceso de auditoría. Pulse Ejecutar una vez ahora para crear el informe. Pulse Ver para ver el informe.
8. Pulse Ejecutar una vez ahora para crear el informe. Pulse Ver para ver el informe.



Este botón Suceso y columnas adicionales aparecerá en todas las tareas de auditoría.

Nota:

Si se ha habilitado la seguridad a nivel de datos observados (consulte valores de Perfil global), entonces se filtrará la salida del proceso de auditoría para que los usuarios sólo vean la información de sus bases de datos.

Bajo las opciones de Informe dentro de Añadir la tarea de auditoría hay dos informes de procedimiento, Sucesos pendientes y Transición del estado del suceso. Añada estos dos informes a dos nuevas tareas de auditoría para mostrar los detalles de todos los sucesos de flujo de trabajo y transiciones. Estos dos informes no se filtrarán (no se aplicará el filtro de seguridad a nivel de datos observado). Estos dos informes están disponibles de forma predeterminada en la lista de informes solo para el usuario administrador y los usuarios con el rol de administración.

Tema principal: Creador de flujos de trabajo

Análisis de detección de amenazas

Guardium incluye un análisis especializado de detección de amenazas que explora y analiza los datos auditados para detectar síntomas que pueden indicar distintos tipos de ataques de base de datos.

El análisis de detección de amenazas explora y analiza los datos auditados para detectar síntomas que puedan indicar ataques de base de datos de procedimientos almacenados o de inyección de SQL. Guardium no se basa en una comparación contra un diccionario en constante cambio de firmas de ataques. En su lugar, Guardium analiza la actividad de datos de auditoría, las excepciones y los datos atípicos (Detección de valores atípicos) durante largos periodos de tiempo en busca de patrones que indican un ataque. Al realizar un seguimiento de los sucesos sospechosos a lo largo del tiempo y correlacionarlos, Guardium crea una imagen global de los riesgos potenciales. Este enfoque es más flexible y completo, y no requiere actualizaciones de firmas continuas.

El análisis de detección de amenazas está soportado en MySQL, Oracle y DB2.

- Características de un ataque de inyección de SQL
- Características de un ataque de procedimientos almacenados
- Habilitación de análisis de detección de amenazas
  En este tema se describen los requisitos previos y los procedimientos para habilitar el análisis de detección de amenazas.
- Cómo trabajar con informes de casos
  Este tema describe cómo trabajar con informes de casos.
- Activación del flujo de trabajo del proceso de auditoría para el análisis de amenazas
  Este procedimiento describe cómo planificar y distribuir los procesos de auditoría necesarios para utilizar las herramientas de diagnóstico de amenazas de Guardium.
- Cómo trabajar con paneles de control de diagnóstico de amenazas
  Un panel de control que se invoca desde un caso de amenaza específico en el informe Sospecha de casos de STP maliciosos o Sospecha de ataque de inyección de SQL se denomina panel de control de diagnóstico de amenazas.
- Funciones de análisis de detección de amenazas

Tema principal: Supervisar y auditar

Características de un ataque de inyección de SQL

Los ataques de inyección de SQL intentan aprovechar las vulnerabilidades de la aplicación web concatenando la entrada del usuario con consultas SQL. Si es satisfactorio, estos ataques pueden ejecutar mandatos SQL maliciosos utilizando la conexión de aplicación web legítima. Los ataques de inyección de SQL pueden ser difíciles de identificar porque los pasos individuales de un ataque, analizados independientemente de otros pasos, pueden considerarse legítimos. Gracias al uso del análisis de detección de amenazas, Guardium identifica posibles ataques de inyección de SQL capturando los pasos individuales y analizándolos como parte de un ataque complejo único.

Los síntomas típicos de ataques de inyección SQL que identifica Guardium son:

- Un atacante que trata de identificar la estructura de una consulta de SQL dinámica, por ejemplo el número de columnas consultadas
- Una cantidad inusualmente grande de nuevas consultas, específicamente consultas que se estructuran de forma exclusiva o inusual
- El acceso a tablas que contienen información sobre la estructura de la base de datos

Tema principal: Análisis de detección de amenazas

Características de un ataque de procedimientos almacenados

Un procedimiento almacenado malicioso es un bloque de código diseñado para evadir la detección y para realizar ataques complejos durante un periodo de tiempo. El ataque exacto se puede repetir, o puede cambiar sus características con el tiempo. El procedimiento almacenado puede estar inactivo durante un periodo de tiempo prolongado, haciendo que sea más difícil identificarlo como sospechoso. Aunque se haya detectado actividad inusual en una auditoría anterior, en el momento en que se produce la siguiente auditoría ya se ha olvidado la actividad anterior. Se puede utilizar un procedimiento almacenado malicioso para ocultar que se haya descartado una tabla importante o para extraer el contenido de una tabla.

Ejemplos de actividad sospechosa son: la creación de un procedimiento almacenado con una sentencia DROP con objetos confidenciales; un verbo DROP; excepciones SQL causadas por objetos que faltan; un procedimiento que se modifica después de estar inactivo durante un periodo de tiempo prolongado.

Guardium realiza un seguimiento de la actividad relacionada con los procedimientos almacenados individuales, y junto con los datos de minería de valores atípicos correlacionan los diversos síntomas y usuarios. Guardium puede detectar estos síntomas típicos de este caso de uso de procedimientos almacenados maliciosos (presentado en el orden en el que se producen normalmente):

1. Un administrador de base de datos crea un Procedimiento A malicioso, que suprime datos de la tabla de clientes
2. Un mes más tarde, el administrador de la base de datos cambia un Procedimiento B utilizado habitualmente para llamar al Procedimiento A
3. Un usuario diferente llama al Procedimiento B modificado, de forma que los datos de la tabla de clientes se suprimen por ese usuario inocente

Tema principal: Análisis de detección de amenazas

Habilitación de análisis de detección de amenazas

En este tema se describen los requisitos previos y los procedimientos para habilitar el análisis de detección de amenazas.

Para habilitar el análisis de detección de amenazas:

- Asegúrese de cumplir con los requisitos mínimos de memoria y almacenamiento necesarios para la búsqueda (4 CPU y 24 GB de RAM).
- Verifique que el sistema tiene datos de aplicación anotados. Concretamente, SQLI requiere datos de aplicación porque la inyección se inicia desde la aplicación. Si el sistema "confía" en la aplicación y no la supervisa en Guardium, la inyección no puede identificarse.
- La detección de valores atípicos no es necesaria para la detección de amenazas de inyección de SQL, pero es necesaria para dar soporte completo a la detección de procedimientos almacenados sospechosos. Para más información, consulte Habilitación e inhabilitación de la detección de valores atípicos localmente en un recopilador.
- Al actualizar a Guardium V10.1 a través del proceso de parches de actualización, debe habilitar la exploración de detección de amenazas en cada recopilador utilizando el mandato de Guardium API: `grdapi enable_advanced_threat_scanning`. Consulte GrdAPI Funciones de detección de amenazas de GuardAPI para obtener más información sobre los parámetros disponibles para el mandato enable_advanced_threat_scanning.
- Configure el proceso de auditoría para enviar informes de casos a los investigadores pertinentes. Es opcional pero se recomienda hacerlo. Consulte Activación del flujo de trabajo del proceso de auditoría para el análisis de amenazas para obtener más información.

Importante: La detección de amenazas se basa en el análisis y la correlación de datos registrados. Por lo tanto, las reglas que filtran el tráfico antes del realizar el registro no se tienen en cuenta para la detección de amenazas. Examine cuidadosamente el uso de las reglas de IGNORE S-TAP SESSION para determinar el riesgo de no registrar estas sesiones en comparación con la optimización de la capacidad del recopilador.

Requisitos previos para el análisis de procedimientos almacenados maliciosos

- El algoritmo de análisis depende en parte de grupos de objetos confidenciales. De forma predeterminada, el algoritmo utiliza miembros en el grupo de objetos confidenciales definido por el sistema (ID de grupo 5). Si ya ha especificado grupos de objetos confidenciales adicionales para la detección de valores atípicos, la detección de amenazas utilizará los mismos grupos. Incluso si la detección de valores atípicos no está habilitada, puede establecer sus propios grupos de objetos confidenciales utilizando el mismo mandato GuardAPI: `set_outliers_detection_parameter parameter_name="sensitiveObjectGroupIds" parameter_value=<ID de grupo>,<ID de grupo>,...`
- Las reglas de política se deben instalar para recopilar el tráfico necesario para el análisis de procedimientos almacenados maliciosos.
  Recomendación: Cree las reglas siguientes en la política en el orden sugerido. Es importante marcar el recuadro de selección Continuar en la siguiente regla para todas estas reglas.
  1. Regla de acceso: Registrar todos los detalles donde el filtro de grupos de mandatos es PROCEDURE DDL.
  2. Regla de acceso: Registrar todos los detalles donde el filtro del grupo de mandatos es mandatos EXECUTE. Si la base de datos es Oracle, incluya el mandato BEGIN en la regla.
  3. Regla de excepción: Solo registrar donde el filtro de tipo de error es SQL_ERROR.

Tema principal: Análisis de detección de amenazas

Cómo trabajar con informes de casos

Este tema describe cómo trabajar con informes de casos.

Guardium analiza los síntomas en el tiempo, los correlaciona y asigna una puntuación por ataque posible identificado. Si la puntuación indica un ataque probable, el conjunto de sucesos pasa a ser un caso cuyo ID es exclusivo por recopilador. Los casos se externalizan en informes de casos, uno por cada ataque sospechoso. Acceda a los informes de casos mediante uno de los siguientes:

- Configure un proceso de auditoría para recibir notificaciones en la lista de tareas pendientes en el gestor central y abra el informe directamente en el recopilador asociado pertinente. Tenga en cuenta que la lista de tareas pendientes se actualiza una vez por hora.
- Acceda a Investigar > Excepciones.

La ventana de informes de casos. Un informe presenta, de forma predeterminada, un máximo de 3 incidencias, una por línea. Cada caso incluye una puntuación de riesgo de 1 a 3, siendo 3 el más grave. Puede:

- Pasar el puntero del ratón sobre el ID de caso para ver un resumen del ataque (solo casos de procedimientos almacenados).
- Pasar el puntero del ratón sobre el ID de caso y pulsar Enlazar a síntomas para acceder al informe de síntomas detallado.
- Pulse el ID para abrir el panel de control de diagnóstico de amenazas específico de caso. Consulte Cómo trabajar con paneles de control de diagnóstico de amenazas.

Restricción: Los informes de casos tienen las restricciones siguientes:

- No hay seguridad a nivel de datos.
- Estos informes no se pueden clonar.
- Puede crear un informe distribuido para estos informes de casos; sin embargo, desde el Gestor central no hay ningún enlace directo desde el informe del caso al panel de control de diagnóstico de amenazas y no hay ninguna ayuda contextual adicional y enlace a síntomas.

Tema principal: Análisis de detección de amenazas

Activación del flujo de trabajo del proceso de auditoría para el análisis de amenazas

Este procedimiento describe cómo planificar y distribuir los procesos de auditoría necesarios para utilizar las herramientas de diagnóstico de amenazas de Guardium.

Acerca de esta tarea

Hay dos procesos de auditoría preconfigurados que controlan la distribución de los informes de análisis de amenazas a los revisores correspondientes:

- Sospecha de casos de STP maliciosos
- Sospecha de casos de inyección de SQL

Cada proceso extrae los casos sospechosos en un tipo de ataque. Puede personalizar estos procesos, o copiar y crear los suyos propios.

Procedimiento

1. Vaya a Cumplir > Herramientas y vistas > Creador de procesos de auditoría. Opcionalmente, filtre los procesos de auditoría disponibles pulsando el botón de selección Sólo inactivos o escribiendo `Sospechoso` en el recuadro Filtro.

   La tarea predeterminada para este proceso es el informe correspondiente (Sospecha de casos de STP maliciosos o Sospecha de casos de inyección de SQL). No modifique los parámetros de ejecución de estos informes. Sin embargo, puede añadir tareas adicionales a este mismo proceso de auditoría. Por ejemplo, puede añadir ambos informes de amenazas a un único proceso de auditoría.

   Si está definiendo estos procesos de auditoría desde un gestor central, defina una tarea para cada recopilador para el que desee ver los datos de amenazas y utilice la opción Origen de datos remoto.

2. Pulse Enviar resultados para definir los receptores del proceso de auditoría que recibirán informes sobre procedimientos almacenados maliciosos sospechosos.
3. Seleccione el receptor predeterminado (usuario) y, a continuación, pulse el icono para definir el receptor o los receptores adecuados para su organización. Cuando haya terminado, pulse Aceptar.
4. Pulse Planificar proceso de auditoría y revise la planificación para el proceso de auditoría.

   La recomendación es ejecutar el proceso cada día, cada hora a partir de las 00:30 horas (una vez que normalmente se ha ejecutado tanto la detección de valores atípicos como la detección de amenazas). Tenga en cuenta que el recuadro de selección Ejecutar automáticamente trabajos dependientes no tiene ningún efecto para esta tarea.

   Importante: Asegúrese de que el recuadro de selección Activar planificación esté seleccionado.
5. Pulse Siguiente y, a continuación, pulse Guardar para terminar de trabajar con el proceso de auditoría.

Tema principal: Análisis de detección de amenazas

Cómo trabajar con paneles de control de diagnóstico de amenazas

Un panel de control que se invoca desde un caso de amenaza específico en el informe Sospecha de casos de STP maliciosos o Sospecha de ataque de inyección de SQL se denomina panel de control de diagnóstico de amenazas.

Un panel de control de diagnóstico de amenazas actúa de forma parecida a otros paneles de control de investigación, excepto que el panel de control para ese caso se rellena con datos de los sucesos sospechosos (usuario de base de datos, servidor, objetos, etc.) y utiliza distintos gráficos para proporcionar vistas diferentes del suceso y sucesos adyacentes que puedan ser útiles para investigar el posible ataque. Los datos de valores atípicos y de búsqueda relevantes también están disponibles en la misma página del panel de control que los gráficos.

En muchos casos, no tendrá que cambiar ninguno de los filtros ya existentes para los paneles de control de diagnóstico de amenazas predefinidos. No obstante, si desea realizar parte de su propio análisis comparativo, puede modificar los filtros ya existentes.

Consulte Panel de control de investigación para obtener más información sobre cómo trabajar con filtros de gráfico y panel de control.

Consejo: El panel de control de diagnóstico de amenazas solo se puede abrir pulsando en el número de caso en el informe de amenazas pertinente. No puede guardar cambios en este panel de control ni en ningún otro panel de control predefinido. Si realiza cambios y desea mantener el panel de control para una investigación adicional, debe copiarlo y guardarlo con un nombre nuevo. También debe guardar los filtros pulsando en el menú Filtros y seleccionando Guardar.

Los datos de referencia son un conjunto de filtros predefinidos específicos de gráficos, solo para Análisis de detección de amenazas, que muestran datos similares al caso que se está investigando pero no se incluyen en el filtro general del panel de control. Los datos de referencia no pueden ser cambiados por los usuarios. Pase el puntero del ratón sobreel icono de filtro en cada gráfico para ver los datos de referencia.

En un escenario típico de sospecha de ataque de inyección de SQL, el panel de control de diagnóstico de amenazas se filtra para este ataque e incluye los siguientes filtros del panel de control generales:

- Servidor: 8.34.223.145
- Usuario de BD: USER1
- Base de datos: 8.4.134.213:31.5.12
- Tipo de BD: MYSQL
- Objeto: stp1_name

El diagrama para el usuario de base de datos puede incluir datos de referencia para usuarios de base de datos similares, como USER2, USER3 y USER4. Esto le permite comparar las actividades del usuario sospechoso con usuarios similares, aunque esos usuarios adicionales no estén incluidos en los filtros generales del panel de control.

No todos los campos incluyen datos de referencia asociados. Cualquier campo para el que no haya ningún filtro de referencia predefinido se filtrará como en el panel de control.

En algunos gráficos, los filtros se pueden desactivar para que pueda comparar los datos independientemente de los filtros elegidos para todo el panel de control. Esto proporciona una imagen más amplia de la actividad.

Pulse el icono de filtro para abrir los valores de filtro de gráfico y realice modificaciones.

- Investigación de amenazas de inyección de SQL
- Investigación de amenazas de procedimientos almacenados

Tema principal: Análisis de detección de amenazas

Investigación de amenazas de inyección de SQL

Acerca de esta tarea

Este procedimiento describe la investigación de un ataque de inyección de SQL sospechoso utilizando el panel de control de diagnóstico de amenazas.

Procedimiento

1. En la lista de tareas pendientes, o desde Investigar > Excepciones, abra el panel de control de Sospecha de casos de inyección de SQL. Cada línea es un caso, con una calificación de confianza de un ataque, y un nivel de riesgo del ataque.
2. Pulse Ver para evaluar si hay falsos positivos. Pase el puntero del ratón sobre el ID de caso seleccionado y pulse Síntomas para abrir la página Síntomas de caso de inyección de SQL. Se describe cada acción sospechosa y se muestra la serie de SQL. Puede ver las modificaciones exactas que el usuario ha realizado en las series. Al avanzar por las distintas series, puede observar cómo el atacante ha obtenido metódicamente más datos utilizando los errores devueltos de consultas anteriores.
3. Pulse el número de ID para abrir el panel de control de diagnóstico predeterminado para ataques de inyección de SQL, que se filtra por la fecha de la incidencia y los detalles de conexión de la aplicación web sospechosos. Esto ayuda a limitar la investigación al tráfico de base de datos que se ha producido durante el ataque. Puede cambiar o descartar el filtro para ampliar el ámbito de la investigación. Utilice la cuadrícula inferior para obtener información más detallada sobre los datos del gráfico. Tenga en cuenta que si se desplaza a un panel de control estándar, se cancelan todos los filtros específicos para el ataque de inyección de SQL.
4. Utilice estas directrices al investigar los gráficos:
   - Cambie la escala de tiempo para buscar picos en el momento del ataque
   - Busque la infracción de cualquier política de seguridad y vea si alguna infracción se correlaciona con otra actividad en el momento del ataque
5. Obtenga detalles mediante el cambio de filtros, periodo de tiempo, etc. para ver si hay diferencias en el sistema.
6. Evalúe los diagramas en el panel de control:

   Recuento de actividades por hora y objeto
   : Este gráfico contiene los objetos de base de datos más utilizados en el momento del ataque. Al expandir el intervalo de tiempo del panel de instrumentos, puede comparar la diferencia en la actividad antes y después del ataque. Pulse una celda si desea filtrar según un objeto determinado. El color indica nombres de objeto diferentes.

   Recuento de errores por tiempo y error
   : Este gráfico indica cuántos errores de SQL han sido generados por la aplicación web. Una tasa alta de errores de SQL puede indicar que se está llevando a cabo algún tipo de ataque de inyección de SQL. El color indica distintos tipos de error.

   Recuento de valores atípicos por tiempo y razón de valor atípico
   : Un ataque de inyección de SQL implica un gran número de consultas nuevas con una estructura distinta a la de las consultas habituales. Esas consultas generan valores atípicos. Utilice este gráfico para ver el volumen y la puntuación de los valores atípicos generados por la aplicación web que ha infringido.

   Recuento de infracciones por tiempo e infracción
   : Durante un ataque de inyección de SQL es probable que el atacante infrinja las políticas de seguridad que registran acceso a objetos no autorizados. Compare el volumen y los tipos de infracciones para comprender el riesgo del ataque.

   Tipos de error sospechosos
   : Utilice este gráfico para explorar errores de SQL específicos que se utilizan en los ataques de inyección de SQL para aprovecharse de la vulnerabilidad. Pulse una celda para filtrar la búsqueda y busque la sentencia SQL que ha generado este error. Es posible que vea un código SQL inyectado.

   Nombres de objetos sospechosos
   : Utilice este gráfico para ver los objetos sospechosos que se utilizan durante los ataques de inyección de SQL. Expanda el periodo de tiempo de la búsqueda para ver si esos objetos se han utilizado antes de que se iniciara el ataque. Compare el volumen del uso de estos objetos.

Tema principal: Cómo trabajar con paneles de control de diagnóstico de amenazas

Investigación de amenazas de procedimientos almacenados

Acerca de esta tarea

Este procedimiento describe la investigación de un ataque de procedimientos almacenados sospechosos, utilizando el panel de control de diagnóstico de amenazas.

Procedimiento

1. En la lista de tareas pendientes, o desde Investigar > Excepciones, abra el panel de control Sospecha de casos de STP maliciosos. Cada línea es un caso, con una calificación de confianza de un ataque, y un nivel de riesgo del ataque.
2. Pulse Ver para evaluar si hay falsos positivos.
3. Pase el puntero del ratón sobre el ID de caso seleccionado para ver los detalles del caso.
4. Pulse los síntomas para abrir la página Síntomas de casos de STP maliciosos.
5. 5. Pulse el número de ID para abrir el panel de control de diagnóstico predeterminado para ataques de inyección de SQL, que se filtra por la fecha de la incidencia y los detalles de conexión de la aplicación web sospechosos. Esto ayuda a limitar la investigación al tráfico de base de datos que se ha producido durante el ataque. Puede cambiar o descartar el filtro para ampliar el ámbito de la investigación. Utilice la cuadrícula inferior para obtener información más detallada sobre los datos del gráfico.
6. Utilice estas directrices al investigar los gráficos:
   - Cambie la escala de tiempo para buscar picos en el momento del ataque
   - Busque la infracción de cualquier política de seguridad y vea si alguna infracción se correlaciona con otra actividad en el momento del ataque
7. Obtenga detalles mediante el cambio de filtros, periodo de tiempo, etc. para ver si hay diferencias en el sistema.
8. Evalúe los diagramas en el panel de control:

   Comparar errores en distintos servidores
   : Utilice este gráfico para comprender si este servidor y usuario de base de datos tienen excepcionalmente más errores que otros usuarios de base de datos.

   Compare errores de distintos usuarios de base de datos con un comportamiento similar
   : Utilice este gráfico para comparar los tipos de error y su volumen en este usuario de base de datos en comparación con usuarios de base de datos similares. Los usuarios de base de datos similares son todos los usuarios que han creado procedimientos almacenados.

   Actividades similares en procedimientos almacenados por este usuario de base de datos
   : Utilice este gráfico para ver los procedimientos almacenados que el usuario ha creado/modificado en el periodo específico. El gráfico se ha filtrado por verbo. Utilice este gráfico también para profundizar más y ver lo que hizo el usuario en los distintos procedimientos almacenados.

   Comparar infracciones de usuarios de base de datos con comportamientos similares
   : Compare el volumen y el tipo de infracción (política) en los usuarios de base de datos que crean procedimientos almacenados.

   Comparar valores atípicos de usuarios de base de datos con comportamientos similares
   : Utilice este gráfico para comparar el volumen y el tipo de valores atípicos de este usuario de base de datos con otros usuarios de base de datos que crean procedimientos almacenados.

   Valores atípicos por fecha en este usuario de base de datos

Utilice este gráfico para ver el volumen y la puntuación de los valores atípicos en el usuario de base de datos específico.

Tema principal: Cómo trabajar con paneles de control de diagnóstico de amenazas

Funciones de detección de amenazas de GuardAPI

enable_advanced_threat_scanning

Habilita procesos de escaneado para comprobar si hay ataques específicos en bases de datos, tales como la inyección de SQL y procedimientos almacenados maliciosos.

Tabla 1. Parámetros de enable_advanced_threat_scanning

Parámetro	Descripción
all	Opcional. Solo en una configuración de gestión central, habilita todos los escaneados de detección de amenazas en todas las unidades gestionadas. Valores permitidos: `true`, `false`.
schedule_start	Opcional. Especifica la fecha y hora para iniciar la ejecución de los procesos. El formato aceptado es aaaa-mm-dd hh:mm:ss (reloj de 24 horas).
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

```
grdapi enable_advanced_threat_scanning all=true schedule_start="2016-03-24 12:00:05”
```

Verá el mensaje siguiente si se ha habilitado el análisis de amenazas, cuando la detección de valor atípico no es:

```
Aviso: Habilitando el escaneo de amenazas avanzado (también conocido como Ojo de águila) cuando la detección de anomalías
analíticas está inhabilitada.
El escaneo de amenazas avanzado (también conocido como Ojo de águila) se ha habilitado.
ok
```

disable_advanced_threat_scanning

Inhabilita el escaneado de detección de amenazas en el explorador.

Tabla 2. Parámetros de disable_advanced_threat_scanning

Parámetro	Descripción
all	Solo en una configuración de gestión central, inhabilita todos los escaneados de detección de amenazas en todas las unidades gestionadas.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

get_eagle_eye_info

Muestra los valores actuales de los parámetros de detección de amenazas.

Tabla 3. Parámetros de get_eagle_eye_info

Parámetro	Descripción

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

```
grdapi get_eagle_eye_info
Eagle Eye Parameters Values:
EI_CASES_DISPLAY_LIMIT = 3
EI_CONFIDENCE_PCT_CHANGE_TO_REDISPLAY_CASE = 30
EI_EAGLE_EYE_ENABLED = 1
EI_PROCESSOR_TIMEOUT_SEC = 420
EI_SCANNER_PATCH_DEF = 10
EI_SCANNER_TIMEOUT_SEC = 300ok
```

set_eagle_eye_parameter

Utilícelo bajo la dirección del personal de IBM. Cambia los parámetros de configuración para la detección de amenazas. Estos parámetros se deben establecer de forma explícita utilizando `parameter_name` y `parameter_value` como se indica a continuación:

```
set_eagle_eye_scanner_parameter parameter_name=[parameter] parameter_value=[value]
```

Tabla 4. Parámetros de set_eagle_eye_parameter

Parámetro	Descripción
EI_CASES_DISPLAY LIMIT	El número de casos que se van a mostrar en el informe de la lista de tareas pendientes. El valor predeterminado es 3.
EI_CONFIDENCE_PCT_CHANGE _TO_REDISPLAY CASE	El porcentaje de cambio de "confianza" que provocará que este caso se vuelva a visualizar en el informe de lista de tareas pendientes, aunque ya se haya incluido antes. Esto puede suceder si Guardium detecta otro síntoma o síntomas que aumentan la confianza con este valor de porcentaje. El valor predeterminado es 30.
EI_PROCESSOR_TIMEOUT_SEC	Los procesadores que se ejecutan durante más tiempo que el valor de este umbral se desactivan. El valor predeterminado es de 420 segundos.
EI_SCANNER_PATCH_DEF	Para evitar falsos positivos como resultado de la instalación de parches, si en una sola ejecución del proceso el número de procedimientos almacenados creados supera este parámetro, el proceso presupone que se ha instalado un parche y detiene el análisis de los síntomas. El valor predeterminado es de 10 creaciones de procedimientos almacenados detectadas en una sola ejecución.
EI_SCANNER_TIMEOUT_SEC	Los procesos de escaneado que se ejecutan durante más tiempo que el valor de este umbral se desactivan. El valor predeterminado es de 300 segundos.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

get_eagle_eye_scanners_info

Devolver información acerca de los valores de escaneado.

Tabla 5. Parámetros de get_eagle_eye_scanners_info

Parámetro	Descripción

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Los datos devueltos contienen la información siguiente:

Tabla 6. Parámetros de get_eagle_eye_scanners_info

Campo	Descripción
ID	El ID del escáner.
Name	El nombre del escáner.
Status	Estado del escáner de la última ejecución: I: En curso D: Hecho K: Interrumpido E: Hecho con errores
Enabled	Indica si está habilitado el escáner. True: Habilitado False: Inhabilitado
Permanent disabled	Si se ha inhabilitado el escáner 3 veces en 24 horas, se inhabilita de forma permanente. True: Inhabilitado False: Habilitado

Ejemplo:

```
grdapi get_eagle_eye_scanners_info
ID=0
ID:1, Name:SQLInjectionExceptionsScanner, Status:D, Enabled:true, Permanent disabled:false
ID:2, Name:NumNewConstructScanner, Status:D, Enabled:true, Permanent disabled:false
ID:3, Name:SQLInjectionSuspiciousObjectScanner, Status:D, Enabled:true, Permanent disabled:false
ID:4, Name:SqliQueryScanner, Status:Unknown, Enabled:false, Permanent disabled:true
ID:5, Name:EagleEyeSTPCreateProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:6, Name:EagleEyeSTPCallProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:7, Name:EagleEyeSTPExceptionProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:8, Name:EagleEyePreviousStpUsageProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:9, Name:EagleEyeSTPViolationProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:10, Name:EagleEyeSTPUserOutlierScanner, Status:D, Enabled:true, Permanent disabled:false
ok
```

set_eagle_eye_scanner_parameter

Utilícelo bajo la dirección del personal de IBM. Activa o desactiva un escáner. Estos parámetros se deben establecer de forma explícita utilizando `parameter_name` y `parameter_value` como se indica a continuación:

```
set_eagle_eye_scanner_parameter parameter_name=[parameter] parameter_value=[value]
```

Tabla 7. Parámetros de set_eagle_eye_scanner_parameter

Parámetro	Descripción
scanner_id	Necesario. El ID exclusivo del escáner, que puede obtener con el mandato de GuardAPI get_eagle_eye_scanners_info.
is_active	Define si el escáner se debe ejecutar. Se utiliza para iniciar un escáner que se ha detenido automático porque ha excedido el tiempo de espera. 0: Se ha detenido el escáner 1: Se ha activado el escáner
is_permanent_inactive	Si se ha inhabilitado el escáner 3 veces en 24 horas, entonces solo se puede volver a habilitar utilizando este mandato de GuardAPI. 1: El escáner se ha detenido de forma permanente 0: El escáner está habilitado

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

El siguiente ejemplo vuelve a activar un escáner desactivado de forma permanente.

```
set_eagle_eye_scanner_parameter scanner_id=2 parameter_name=is_permanent_inactive parameter_value=0
```

get_eagle_eye_symptom_period_hours

Mostrar el valor del parámetro de periodo de sistema en horas. El periodo de síntoma determina durante cuánto tiempo el proceso está buscando y analizando los síntomas recopilados para un caso.

Tabla 8. Parámetros de get_eagle_eye_symptom_period_hours

Parámetro	Descripción
case_name	Necesario. El tipo de caso. Se permiten los valores siguientes: STP: Caso de procedimiento almacenado malicioso SQL_INJECTION: Caso de inyección de SQL
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

```
grdapi get_eagle_eye_symptom_period_hours case_name=STP
The symptoms period for case type: STP is: 168 in hours
ok
```

set_eagle_eye_symptom_period_hours

Establece un valor para el parámetro de periodo de sistema en horas. El periodo de síntoma determina durante cuánto tiempo el proceso está buscando y analizando los síntomas recopilados para un caso.

Tabla 9. Parámetros de set_eagle_eye_symptom_period_hours

Parámetro	Descripción
case_name	Necesario. El tipo de caso. Se permiten los valores siguientes: STP: Caso de procedimiento almacenado malicioso SQL_INJECTION: Caso de inyección de SQL
symptom_period_hours	Necesario. Entero. El número de horas anteriores para analizar los síntomas de un caso.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

```
grdapi set_eagle_eye_symptom_period_hours case_name=STP symptom_period_hours=170
The symptoms period for case type: STP was changed. The old value was: 168. The new value is: 170
ok
```

get_eagle_eye_debug_level

Para uso del personal de IBM. Muestra el nivel de depuración actual:

- 1: Activado
- 0: Desactivado

Tabla 10. Parámetros de get_eagle_eye_debug_level

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

```
grdapi get_eagle_eye_debug_level
ID=0
component=EAGLE_EYE level=1
ok
```

set_eagle_eye_debug_level

Para uso del personal de IBM. Muestra el nivel de depuración actual.

Tabla 11. Parámetros de set_eagle_eye_debug_level

Parámetro	Descripción
level	Entero. Necesario. Valores permitidos: 1: Activado 0: Desactivado
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

```
grdapi set_eagle_eye_debug_level level=0
ID=0
ok
```

Tema principal: Referencia de GuardAPI

Panel de control de investigación

El Panel de control de investigación proporciona potentes herramientas para identificar y evaluar problemas que pueden existir en el entorno de Guardium. Utiliza datos sin filtrar locales o de todo el sistema, y proporciona numerosas opciones de filtro para consultar datos en todo un entorno de Guardium, potencialmente desde cualquier recopilador de Guardium dentro de dicho entorno.

El panel de instrumentos de investigación proporciona gráficos interrelacionados que ayudan a revelar patrones, anomalías y relaciones entre los datos. No requiere un conocimiento detallado de los esquemas de topología, agregación o equilibrio de carga. Contiene la búsqueda rápida original de funciones de empresa y otras herramientas para visualizar y analizar datos.

Nota: Se recomienda ver el panel de control de investigación en modalidad de pantalla completa.
Restricción: El panel de control de investigación y la seguridad a nivel de datos no se puede habilitar simultáneamente.

Modalidad de operación

El panel de control de investigación da soporte a tres modalidades de operación:

Solo Gestor central

Las consultas se envían a un Gestor central que devuelve resultados de toda la empresa desde todos los recopiladores de Guardium con la búsqueda habilitada. Las consultas que se envían en unidades gestionadas devuelven resultados locales.

Solo Gestor central es la modalidad de operación predeterminada.

Todas las máquinas

Las consultas de búsqueda en toda la empresa se envían desde cualquier máquina en el entorno de Guardium con la búsqueda habilitada. Esta modalidad puede generar resultados de búsqueda más lentos y requiere conectividad entre todas las unidades gestionadas del entorno.

Solo local

Esta modalidad limita consultas de búsqueda en el recopilador local donde se envía la búsqueda: no se recupera ningún dato de otros recopiladores en el entorno de Guardium. En un Gestor central en modalidad solo local, no hay ningún dato visualizado.

Consulte Búsqueda rápida de GuardAPI para funciones de empresa para obtener información sobre cómo establecer la modalidad de búsqueda.

Componentes del panel de control

Un panel de control es una recopilación de uno o más de los siguientes elementos:

- Gráficos de datos de tres ejes, conocidos como gráficos trimétricos. Estos gráficos se pueden visualizar como un mapa de colores, gráfico de barras, gráfico de burbujas, gráfico de líneas, gráfico circular, gráfico de pasos y gráfico de áreas.
- Gráfico de burbujas animadas: Una visualización animada de los cambios de datos en las últimas 48 horas.
- Gráfico de actividades: Un gráfico de líneas que visualiza el volumen de actividad y valores atípicos. Se localiza encima de la Tabla de resultados.
- Tabla de resultados: Proporciona los resultados de búsqueda y las características de investigación de la búsqueda rápida original. La tabla de resultados siempre está en la parte inferior del panel de control. Puede añadirse a cualquier panel de control.
- Lista de facetas de una o más de Dónde, Quién, Qué, Excepción y Cuándo. Aparece en el lado izquierdo de cada panel de control y no se puede eliminar.

Existen cuatro vistas predeterminadas de DAM y dos vistas predeterminadas de FAM, cada una con diferentes gráficos y tablas. Seleccione la vista en el menú del panel de control . Las vistas predeterminadas no se pueden modificar.

- Habilitación e inhabilitación del panel de control de investigación
  Este tema describe cómo habilitar e inhabilitar el panel de control de investigación.
- Habilitación de actividad de archivos en el panel de control de investigación
- Acceso al panel de control de investigación
- Panel de control de investigación para datos
  El panel de control de investigación es un grupo preestablecido de gráficos y una tabla que le ayudan a comprender lo que sucede en el sistema en un momento determinado, y en el que puede crear sus propios paneles de control personalizados.
- Panel de control de investigación para archivos
  El panel de control de investigación es un grupo preestablecido de gráficos y una tabla que le ayudan a comprender lo que sucede en el sistema en un momento determinado, y en el que puede crear sus propios paneles de control personalizados.
- Filtrado de datos y guardado de filtros en el panel de control de investigación
- Filtrado de un gráfico individual
- Creación, guardado y exportación de paneles de control de investigación
- Utilización de la vista de topología
  La vista de topología es la visualización de los dispositivos de Guardium en los resultados de la búsqueda.
- Búsqueda local y distribuida
- Utilización de visión de datos
  La visualización Visión de datos permite al usuario examinar profundamente una secuencia de sucesos que son capturados por el sistema Guardium. Proporciona una imagen completa de la actividad en un intervalo de tiempo específico y ayuda a detectar comportamientos inusuales.

Tema principal: Supervisar y auditar
Información relacionada:
Funciones del panel de control de investigación de GuardAPI
Mandatos de CLI del panel de control de investigación

Habilitación e inhabilitación del panel de control de investigación

Este tema describe cómo habilitar e inhabilitar el panel de control de investigación.

Antes de empezar

El panel de control de investigación tiene los siguientes requisitos de hardware mínimos:

- Arquitectura de 64 bits
- 24 GB de RAM
- CPU de 4 núcleos

Restricción: El panel de control de investigación y la seguridad a nivel de datos no pueden estar habilitados simultáneamente.

Acerca de esta tarea

Los pasos descritos a continuación le permiten habilitar o inhabilitar la búsqueda.

Procedimiento

1. Inicie la sesión en la máquina como usuario o administrador con el rol de CLI.
2. Utilice el siguiente mandato GuardAPI para habilitar el panel de control de investigación:

   ```
   grdapi enable_quick_search schedule_interval=2 schedule_units=MINUTE
   ```

   De forma predeterminada, las infracciones no se incluyen en los resultados de búsqueda. Para incluir infracciones, establezca el parámetro includeViolations en `true`:

   ```
   grdapi enable_quick_search schedule_interval=2 schedule_units=MINUTE includeViolations=true
   ```

   Para habilitar la detección de valores atípicos, consulte Detección de valores atípicos.

   Pueden especificarse parámetros adicionales como, por ejemplo, el intervalo de actualización del índice de búsqueda. Para obtener una lista completa de parámetros y descripciones, consulte la información de referencia de Funciones del panel de control de investigación de GuardAPI.

3. Utilice el mandato GuardAPI siguiente para inhabilitar la función de panel de control de investigación en cualquier momento:

   ```
   grdapi disable_quick_search
   ```

Resultados

Una vez habilitado, consulte Acceso al panel de control de investigación para obtener más información y empezar a utilizar el panel de control de investigación.

Atención:

- La funcionalidad del panel de control de investigación abre los puertos8983 y 9983 tanto en gestores centrales como en los recopiladores. Los puertos se abren cuando el panel de control de investigación está habilitado y se cierra cuando está inhabilitado. Para utilizar el panel de control de investigación, asegúrese de que la comunicación bidireccional entre los gestores y los recopiladores en los puertos 8983 y 9983 no esté bloqueada por ningún cortafuegos.
- Los datos de búsqueda indexada se retienen durante 3 días. Utilice el mandato de CLI de Guardium de objeto de depuración para cambiar el periodo de retención. Por ejemplo, el siguiente mandato cambia el periodo de retención a 5 días: store purge object age 39 5. Tenga en cuenta que `39` es el número de identificación de objeto predeterminado asociado al índice de búsqueda. Para obtener información adicional, consulte la información de referencia de Mandatos de CLI de configuración y control.

Tema principal: Panel de control de investigación
Información relacionada:
Funciones del panel de control de investigación de GuardAPI
Mandatos de CLI del panel de control de investigación

Habilitación de actividad de archivos en el panel de control de investigación

Antes de empezar

- El lote de FAM debe estar instalado y configurado. Consulte Parámetros GIM de descubrimiento y clasificación de archivos
- El panel de control de investigación debe estar habilitado. Consulte Habilitación e inhabilitación del panel de control de investigación
- No utilice el rastreador FAM V10.1 con el sistema V10.0 Guardium. No utilice el rastreador FAM V10.0 con el sistema V10.1 Guardium.

Acerca de esta tarea

Nota: FAM consulta el servidor para las direcciones IP de servidor y toma la primera que encuentra. No hay ninguna forma de seleccionar la dirección IP adecuada desde un nombre de host cuando el host tiene varias direcciones IP. Los clientes deben especificar la dirección IP de forma explícita si desean estar garantizadas para ver dicha dirección IP en los informes.

Procedimiento

1. En el recopilador , en el indicador de interfaz de línea de mandatos, ejecute el mandato GuardAPI:
   `grdapi enable_fam_crawler [extraction_start] [schedule_start] [activity_schedule_interval] [activity_schedule_units] [entitlement_schedule_interval] [entitlement_schedule_units]` Ejemplo: El mandato siguiente envía los resultados actualizados de descubrimiento y clasificación a Enterprise Search para los datos de clasificación cada 2 minutos y para la información de titularidad cada día.
   `grdapi enable_fam_crawler activity_schedule_interval=2 activity_schedule_units=MINUTE entitlement_schedule_interval=1 entitlement_schedule_units=DAY`
   De forma predeterminada, la extracción se inicia al especificar el mandato, extrayendo datos desde el momento (hora) en que se ha especificado el mandato.
2. Repita en cada recopilador.

Tema principal: Panel de control de investigación
Conceptos relacionados:
Panel de control de investigación para archivos
Información relacionada:
Funciones del panel de control de investigación de GuardAPI

Acceso al panel de control de investigación

Procedimiento

1. Pulse Investigar > Buscar actividad de datos o Investigar > Buscar actividad de archivos.
2. También puede conmutar la búsqueda a Interfaz de usuario y buscar en el panel de control de investigación. A continuación, seleccione Buscar actividad de datos o Buscar actividad de archivos.

Resultados

Se abre el panel de control de investigación predeterminado para los datos o los archivos. De forma predeterminada, el único filtro que se aplica a todo el panel de control es para mostrar la última hora de datos.
Tema principal: Panel de control de investigación

Panel de control de investigación para datos

El panel de control de investigación es un grupo preestablecido de gráficos y una tabla que le ayudan a comprender lo que sucede en el sistema en un momento determinado, y en el que puede crear sus propios paneles de control personalizados.

Existen cuatro vistas predeterminadas para la supervisión de la actividad de datos, cada una con gráficos y tablas diferentes. Seleccione la vista en el menú del panel de control . Las vistas predeterminadas no se pueden modificar.

Los paneles de control predeterminados contienen datos de la última hora presentados en uno o varios de:

- Gráficos trimétricos (gráficos de datos de 3 ejes). La vista predeterminada es un mapa de colores. Las vistas adicionales son gráfico de barras, gráfico de burbujas, gráfico de líneas, gráfico circular, gráfico de pasos y gráfico de áreas.
- Tabla de resultados: Proporciona los resultados de búsqueda y las características de investigación de la búsqueda rápida original. La tabla de resultados siempre está en la parte inferior del panel de control. Puede añadirse a cualquier panel de control. Los separadores son:
  - Actividad: Separadores Resumen y Detalles. Cada fila en el separador Resumen ofrece el número de instancias de actividades registradas por servidor: par de BD y el número de tipos de BD. El Resumen detallado añade el recuento de Programas fuente, Usuarios de BD, Usuarios de SO, Nombre de host del cliente, IP de cliente y fecha. Cada fila en el separador Detalles ofrece detalles completos sobre una actividad.
  - Valores atípicos: Consulte Interpretación de valores atípicos de datos en el panel de control de investigación
  - Errores: Separadores Resumen y Detalles. Cada fila del separador Resumen proporciona el número de instancias de errores notificados por el servidor y el número de tipos de BD de usuarios de BD. El Resumen detallado añade el IPS de cliente, tipos de error y fechas. Cada fila del separador Detalles proporciona detalles completos sobre un error.
  - Infracciones: Separadores Resumen y Detalles. Cada fila en el separador Resumen ofrece el número de instancias de infracciones registradas por servidor: par de BD y el número de tipos de BD. El Resumen detallado añade el recuento de programas fuente, usuarios de BD, usuarios de SO, nombre de host de cliente, IP de cliente, gravedad, infracción y fecha. Cada fila del separador Detalles proporciona detalles completos sobre una infracción.

Las vistas adicionales que puede añadir o abrir son:

- Vista de topología Buscar vista de estado del servidor: consulte Utilización de la vista de topología
- Gráfico de burbujas animadas: Una visualización animada de los cambios de datos en las últimas 48 horas. El gráfico muestra el comportamiento de los objetos durante un periodo de 24 horas. Cada objeto se representa como un círculo, y su área y posición (eje x y y) representan tres variables seleccionadas por el usuario. La animación representa el comportamiento del objeto a lo largo de las 24 horas. Acceda desde la lista desplegable Añadir gráfico.
- Gráfico de actividades: Un gráfico de líneas que visualiza el volumen de actividad y los valores atípicos, situado encima de la tabla de resultados. Acceda desde la lista desplegable Añadir gráfico.
- Visión de datos: Visualización en 3-D de actividad de datos, consulte Utilización de visión de datos. Acceda desde la lista desplegable Añadir gráfico.

Controle y opciones en esta página:

- Una lista de facetas categorizadas de Dónde, Quién, Qué, Excepción y Cuándo, de los resultados de la búsqueda aparece en el lado izquierdo de cada panel de control y no se puede eliminar. Filtre todo el panel de control según las facetas específicas expandiendo la lista y pulsando facetas individuales.
- La fila Filtros activos situada en la parte superior de la ventana muestra los filtros actuales. Suprima los filtros pulsando la .
- Campo de búsqueda: Búsqueda de texto libre que filtra los resultados en todos los campos simultáneamente, independientemente de la faceta
- Búsqueda distribuida: consulte Búsqueda local y distribuida
- Periodo de tiempo para el que se presentan los datos: Modifique pulsando el desplegable en la esquina superior derecha. Las opciones son la última hora, las últimas 3 horas, el último día, los últimos 3 días, cualquier periodo de tiempo que especifique. El valor predeterminado es una hora.
- Desplegable de filtros: Consulte Filtrado de datos y guardado de filtros en el panel de control de investigación
- añadir nuevo panel de control guardar cambios en el panel de control guardar panel de control como: consulte Creación, guardado y exportación de paneles de control de investigación

Tema principal: Panel de control de investigación
Conceptos relacionados:
Interpretación de valores atípicos de datos en el panel de control de investigación
Tareas relacionadas:
Utilización de la vista de topología
Utilización de visión de datos

Panel de control de investigación para archivos

El panel de control de investigación es un grupo preestablecido de gráficos y una tabla que le ayudan a comprender lo que sucede en el sistema en un momento determinado, y en el que puede crear sus propios paneles de control personalizados.

Hay dos vistas de FAM predeterminadas, cada una con diferentes gráficos y tablas. Seleccione la vista en el menú del panel de control . Las vistas predeterminadas no se pueden modificar.
Nota: La IP de servidor y la IP de cliente son siempre las mismas en el panel de control, excepto en el caso de la conexión a través del escritorio remoto en Windows. La IP de cliente solo está soportada cuando se conecta a través de una sesión de escritorio remoto.
Nota: FAM consulta el servidor para las direcciones IP de servidor y toma la primera que encuentra. No hay ninguna forma de seleccionar la dirección IP adecuada desde un nombre de host cuando el host tiene varias direcciones IP. Especifique la dirección IP de forma explícita si desea que se le garantice ver dicha dirección IP en los informes.
Los paneles de control predeterminados contienen datos de la última hora presentados en uno o varios de:

- Gráficos trimétricos (gráficos de datos de 3 ejes). La vista predeterminada es un mapa de colores. Las vistas adicionales son gráfico de barras, gráfico de burbujas, gráfico de líneas, gráfico circular, gráfico de pasos y gráfico de áreas.

- Tabla de resultados: Proporciona los resultados de búsqueda y las características de investigación de la búsqueda rápida original. La tabla de resultados siempre está en la parte inferior del panel de control. Puede añadirse a cualquier panel de control. Los separadores son:
    - Actividad: separadores Resumen y Detalles que muestran los datos supervisados, en función de las reglas de política del servidor de archivos. Cada fila del separador Resumen proporciona el número de instancias de actividades de acceso registradas por servidor y usuario de SO. El separador Detalles añade el Nombre de host del servidor, Servidor, Nombre de host del cliente, IP de cliente, Usuario de SO, Nombre de archivo completo, Mandato, Fecha y Hora. Cada fila en el separador Detalles ofrece detalles completos sobre una actividad. Los datos del separador Actividad son coherentes con la fecha y la hora del recopilador.
    - Valores atípicos: consulte Interpretación de los valores atípicos de actividad de archivos
    - Errores: Separadores Resumen y Detalles. Cada fila del separador Resumen proporciona el número de instancias de errores notificados por el IP de servidor y cliente, y la fecha. El Resumen detallado añade los detalles del error y la hora. Cada fila del separador Detalles proporciona detalles completos sobre un error.
    - Infracciones: Separadores Resumen y Detalles. Cada fila del separador Resumen proporciona el número de instancias de infracciones registradas por servidor, programa fuente y combinación de usuario de sistema operativo. El Resumen detallado añade la IP de cliente, la gravedad, la infracción y los detalles de la infracción, fecha y hora. Cada fila del separador Detalles proporciona detalles completos sobre una infracción. Los datos del separador Infracciones son coherentes con los datos y la hora del servidor de archivos.
    - Titularidad: Separadores Resumen y Detalles. Para los servidores de archivos, este separador presenta datos confidenciales basados en los planes de decisiones de FAM actuales. Cada fila del separador Resumen proporciona el número de instancias de actividades de acceso registradas por servidor y propietario. El separador Detalles añade el nombre de host del servidor, la vía de acceso completa, el tipo, , el tamaño, las entidades de clasificación (el plan de decisiones que ha provocado que este archivo se identifique como confidencial), el propietario, el nombre de host de cliente, la IP de cliente, el usuario de SO, el nombre completo de archivo, los usuarios y grupos con permisos de escritura, lectura, ejecución y supresión, la última modificación, la versión (sólo Sharepoint), hora de creación, fecha y hora. Cada fila en el separador Detalles ofrece detalles completos sobre una actividad. Puede utilizar los datos de esta tabla para crear grupos y reglas de política para los servidores de archivos; consulte Creación de una regla de política de FAM desde el separador de titularidades del Panel de control de investigación.

Las vistas adicionales que puede añadir o abrir son:

- Vista de topología Buscar vista de estado del servidor: consulte Utilización de la vista de topología
- Gráfico de burbujas animadas: Una visualización animada de los cambios de datos en las últimas 48 horas. El gráfico muestra el comportamiento de los objetos durante un periodo de 24 horas. Cada objeto se representa como un círculo, y su área y posición (eje x y y) representan tres variables seleccionadas por el usuario. La animación representa el comportamiento del objeto a lo largo de las 24 horas. Acceda desde la lista desplegable Añadir gráfico.
- Gráfico de actividades: Un gráfico de líneas que visualiza el volumen de actividad y los valores atípicos, situado encima de la tabla de resultados. Acceda desde la lista desplegable Añadir gráfico.

Controle y opciones en esta página:

- Una lista de facetas categorizadas de Dónde, Quién, Qué, Excepción y Cuándo, de los resultados de la búsqueda aparece en el lado izquierdo de cada panel de control y no se puede eliminar. Filtre todo el panel de control según las facetas específicas expandiendo la lista y pulsando facetas individuales.
- La fila Filtros activos situada en la parte superior de la ventana muestra los filtros actuales. Suprima los filtros pulsando el botón .
- Campo de búsqueda: Búsqueda de texto libre que filtra los resultados en todos los campos simultáneamente, independientemente de la faceta
- Búsqueda distribuida: consulte Búsqueda local y distribuida
- Periodo de tiempo para el que se presentan los datos: Modifique pulsando el desplegable en la esquina superior derecha. Las opciones son la última hora, las últimas 3 horas, el último día, los últimos 3 días, cualquier periodo de tiempo que especifique. El valor predeterminado es una hora.
- Desplegable de filtros: Consulte Filtrado de datos y guardado de filtros en el panel de control de investigación
- añadir nuevo panel de control guardar cambios en el panel de control guardar panel de control como: consulte Creación, guardado y exportación de paneles de control de investigación

Tema principal: Panel de control de investigación
Conceptos relacionados:
Interpretación de los valores atípicos de actividad de archivos
Tareas relacionadas:
Utilización de la vista de topología

Filtrado de datos y guardado de filtros en el panel de control de investigación

Acerca de esta tarea

Puede filtrar datos en todo el panel de control de investigación y en un gráfico individual. Puede profundizar más desde la tabla de resultados hasta la información relacionada.

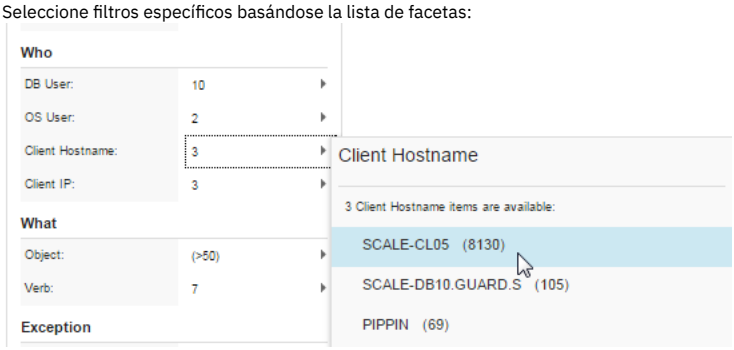
Puede guardar filtros para su uso futuro. Cuando guarda un conjunto de filtros, puede elegir si desea compartirlo y elegir los roles con los que lo comparte.

Procedimiento

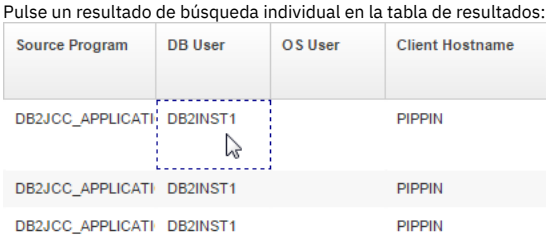
1. Utilice las reglas y la sintaxis para filtrar datos:
    - Para hacer coincidir una frase exacta, utilice comillas dobles alrededor de los términos de búsqueda. Por ejemplo, “Lista de alertas de perfilado” devuelve entradas para Lista de alertas de perfilado de conexión pero no para Alerta de lista de perfilado.
    - Para hacer coincidir todos los términos de búsqueda especificados, separe los términos con un espacio. Por ejemplo, getlisting de Hadoop devuelve todas las entradas que contenga tanto Hadoop como getlisting en cualquier ubicación o secuencia.
    - Para hacer coincidir los términos de búsqueda especificados, separe los términos con OR o una barra vertical (|). Por ejemplo, Hadoop OR getlisting devuelve todas las entradas que contienen Hadoop o getlisting en cualquier ubicación.
    - Para excluir un término de búsqueda especificado, utilice NOT o un punto (.) . Por ejemplo, NOT Hadoop no devuelve ninguna entrada que contenga Hadoop en alguna ubicación.
    - Se da soporte a los caracteres comodín utilizando asteriscos (*) al principio o al final de una serie. Por ejemplo, 10.10.70.* devuelve todas las entradas con la serie 10.10.70. seguida de cualquier carácter adicional.
    - Las reglas de búsqueda se pueden combinar. Por ejemplo, 2016–5-08 (19.*|20.*) devuelve resultados en el rango de tiempo del 8 de mayo entre las horas de 19:00:00 – 20:59:59.

   La adición de filtros cambia cada vista en función del valor de *RefFilter* especificado para la vista. Los filtros actuales aparecen en la barra de menús. Cada uno puede borrarse pulsando su X.

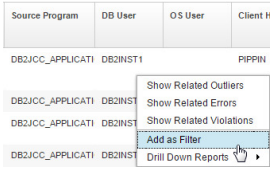
2. Refina los resultados de búsqueda con cualquiera de los siguientes métodos:
   - Seleccione filtros específicos basándose la lista de facetas:



   - Pulse las cabeceras de ejes x o y del gráfico.
   - Pulse un resultado de búsqueda individual en la tabla de resultados:



   Nota: Puede seleccionar una o más filas y pulsar con el botón derecho del ratón en una de las celdas de servidor/usuario de BD/IP de cliente para añadirlas a un grupo existente, o para crear un grupo nuevo.
3. Profundice por los resultados individuales pulsando el botón derecho del ratón en los resultados de búsqueda específicos y explorando valores atípicos, errores o infracciones, o visualizando uno de varios informes desplegables disponibles.



4. Para guardar un conjunto de filtros, pulse Filtros > Guardar. Proporcione un nombre para el filtro y márquelo como Privado o pulse Compartir con para compartir el filtro con roles específicos. Para guardarlo como conjunto de filtros predeterminado (el panel de control siempre se abre con estos filtros), seleccione Establecer como filtro predeterminado. Cuando haya terminado, pulse Aceptar para guardar el filtro.

Tema principal: Panel de control de investigación

Filtrado de un gráfico individual

Acerca de esta tarea

Puede filtrar un gráfico individual. El icono se vuelve rojo cuando se establecen filtros específicos para un gráfico que son diferentes a los filtros de panel de control generales. Pase el puntero del ratón sobre el icono para ver qué filtros se utilizan en ese gráfico.

Un gráfico puede tener un conjunto de filtros como inactivo, lo que significa que los datos del gráfico no se filtran por ese campo. Esto permite a Guardium visualizar otros elementos, además de los relacionados con el caso, que pueden ser similares o de algún modo proporcionar información adicional sobre la investigación.
Ejemplo: Mientras se investiga la actividad de un servidor, se desea comparar uno de los gráficos con los datos de otros servidores. Esto es posible desactivando el filtro Servidor solo para ese gráfico. Para ello, debe pulsar el icono y seleccione el botón de selección Inactivo para la fila Servidor.

Procedimiento

1. Pulse el icono . Se abre Valores de filtro de gráfico.
2. Marque o desmarque los botones de radio según proceda y pulse Aplicar.

Tema principal: Panel de control de investigación

Creación, guardado y exportación de paneles de control de investigación

Acerca de esta tarea

Hay muchas formas de filtrar los datos en el panel de control. Los conjuntos de filtros pueden ser privados o compartidos. Por ejemplo, una persona que está familiarizado con el entorno puede configurar filtros. Esta persona puede crear los filtros para un investigador específico y luego compartir el filtro con dicho rol. No puede cambiar y guardar los paneles de control del sistema predefinidos bajo sus nombres originales.
Importante: Todos los paneles de control de investigación son públicos. Cuando se guarda un panel de control, todos los usuarios que tienen acceso a los paneles de control también tienen acceso al panel de control guardado a través del menú de panel de control. Además, si guarda un panel de control como el panel de control predeterminado, todos los usuarios verán ese valor predeterminado.
Puede utilizar los mismos paneles de control con conjuntos de filtro distintos, en función de qué datos desee ver.
Ejemplo: El panel de control incluye un gráfico de actividad que muestra las actividades de los usuarios de base de datos con un desglose por IP de cliente. Desea ver los mismos datos filtrados por distintas bases de datos, como por ejemplo RRHH frente a Financiero. Es posible que desee añadir también tipos de mandatos diferentes para cada base de datos.

- Filtro 1: por base de datos HR, por verbo SELECT
- Filtro 2: por base de datos FINANCIAL, por verbo UPDATE

Puede abrir el mismo panel de control y conmutar entre los distintos conjuntos de filtros asociados a ese gráfico utilizando los iconos y situados encima de la lista Filtros activos.

Los paneles de control de investigación, incluidos los diagnósticos de amenazas, se pueden cifrar y exportar para su uso compartido. Sólo se exportan las definiciones de panel de control, no los filtros.

Si tiene un panel de control que está configurado con un buen conjunto de gráficos para investigar tipos de incidencias concretas, puede compartir este conocimiento con otros usuarios de Guardium sin incluir datos de ataque reales ni revelar los filtros.

Procedimiento

1. Para guardar la visualización actual, pulse el icono .
2. Para guardar un panel de control con un nombre diferente para su modificación y uso subsiguiente, pulse el icono y guárdelo con un nombre descriptivo y, opcionalmente, una categoría. También puede definir una categoría al guardar el panel de control. El nombre y la categoría pueden incluir espacios. Para recuperar el panel de control más adelante, pulse el icono para abrir el menú del panel de control.
3. Para exportar paneles de control de investigación, vaya a Gestionar > Gestión de datos > Exportar definiciones. En el menú Tipo, seleccione Panel de control de investigación y seleccione las definiciones de panel de control a exportar. A continuación, pulse Exportar.

Tema principal: Panel de control de investigación

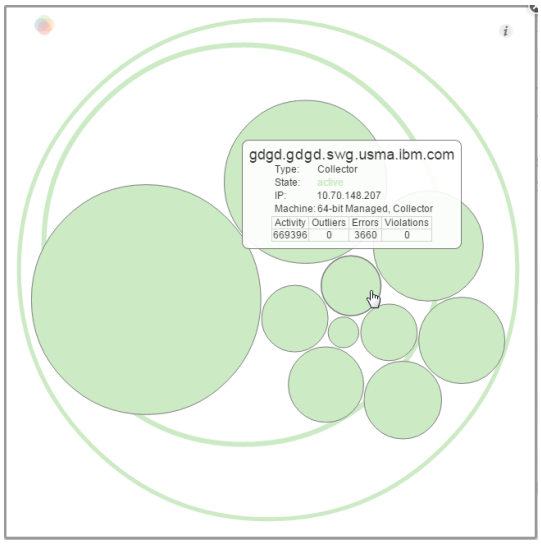
Utilización de la vista de topología

La vista de topología es la visualización de los dispositivos de Guardium en los resultados de la búsqueda.

Acerca de esta tarea

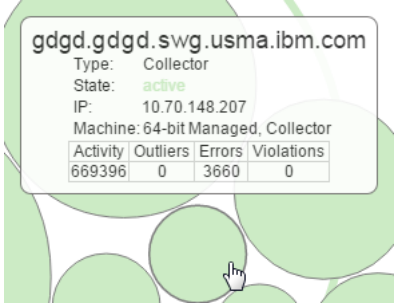
Puede ver detalles sobre cada servidor, seleccionar criterios de filtro, acotar los resultados de búsqueda a segmentos específicos del entorno de Guardium global. Los círculos sólidos representan a recopiladores y agregadores. Los círculos esbozados representan a los gestores. El color del círculo indica el estado del servidor. El color de contorno del Gestor central indica su estado. El tamaño del círculo indica el volumen relativo de los datos recopilados.

La vista de topología no está soportada en máquinas autónomas.



Procedimiento

1. Para abrir la vista de topología, pulse el icono Vista de estado de servidor de búsqueda Vista de estado de servidor de búsqueda en la barra de herramientas del panel de control de investigación.
2. Pase el ratón por encima de un objeto para visualizar información detallada sobre dicho objeto.



3. Seleccione un objeto para acotar los resultados de la búsqueda a solo ese objeto y sus hijos, si existe alguno. Utilice Control + pulsación para seleccionar o deseleccionar varios objetos en la vista de topología.
4. Cierre la vista de topología pulsando el icono de cierre o pulsando fuera del navegador de topología. Los resultados de la búsqueda se actualizan automáticamente para que reflejen los datos disponibles en función del ámbito seleccionado en la vista de topología.

Tema principal: Panel de control de investigación

Búsqueda local y distribuida

Acerca de esta tarea

Los paneles de control de investigación pueden ejecutarse en modalidades distribuidas o locales. En modalidad local, las búsquedas estarán limitadas a los datos disponibles bajo la máquina local (la máquina desde la que se ejecuta la búsqueda). Por ejemplo, una búsqueda local que se ejecuta desde un recopilador individual devuelve resultados de los orígenes de datos bajo dicho recopilador, pero no de los orígenes de datos de otros recopiladores del entorno. En la modalidad distribuida, las búsquedas devuelven datos de todo el entorno de Guardium y los resultados no están limitados por la máquina específica en la que se ejecuta la búsqueda. Se proporciona una herramienta de topología para reducir de forma práctica los resultados de búsqueda a segmentos específicos del entorno de Guardium global.

El valor predeterminado de los paneles de control de investigación es el modo de búsqueda local.

Procedimiento

1. Para conmutar entre la búsqueda local o distribuida, pulse el icono Habilitar / Inhabilitar Buscar en todos los dispositivos en la barra de herramientas de la ventana de búsqueda. Los resultados de la búsqueda se actualizan automáticamente para reflejar los datos disponibles basándose en la selección de la búsqueda local o distribuida.
2. Consulte Utilización de la vista de topología para obtener información sobre los resultados de búsqueda globales de filtrado por un segmento específico del entorno de Guardium.

Tema principal: Panel de control de investigación

Utilización de visión de datos

La visualización Visión de datos permite al usuario examinar profundamente una secuencia de sucesos que son capturados por el sistema Guardium. Proporciona una imagen completa de la actividad en un intervalo de tiempo específico y ayuda a detectar comportamientos inusuales.

Acerca de esta tarea

Visión de datos introduce un paradigma revolucionario que utiliza prestaciones visuales humanas para obtener una visión general de las transacciones de datos e identificar comportamientos inesperados. Guardium ya proporciona sólidas características de análisis de datos y aprendizaje máquina para ayudar en auditorías y para detectar ataques. Los algoritmos, el análisis de datos y los gráficos se han diseñado en base a la experiencia y el conocimiento acumulados. La visión de datos utiliza la flexibilidad de la percepción de la visión humana para detectar asociaciones y movimientos en los datos en bruto que no se ajustan a un patrón de ataques conocidos que de otra forma pasarían desapercibidos. La herramienta presenta diversos aspectos de los datos en un escenario visual complejo, y proporciona al observador herramientas para explorar directamente grandes cantidades de datos complejos.

La visión de datos convierte datos auditados a una visualización cronológica de 3-D del flujo de datos, de orígenes a destinos, mostrando como se van realizando las transacciones exactamente tal como se producen.

El espacio de visualización contiene dos planos, cada uno representa entidades del dominio de auditoría de un tipo específico. Cada entrada de los datos de auditoría se representa como una 'línea parpadeante' que se mueve de un objeto del plano superior (por ejemplo, las IP de cliente) a un objeto del plano inferior (por ejemplo, bases de datos). La línea parpadeante entre el origen y el destino deja un camino (una línea punteada) que indica la presencia de la interacción entre el origen y el destino específicos, que gradualmente se desvanece en el fondo. Los caminos proporcionan una visión general de la interacción entre los orígenes y los destinos en el periodo de tiempo seleccionado. El tamaño de cada origen y destino es relativo a su nivel de actividad. Los orígenes están ubicados cerca de sus destinos y cerca de otros orígenes similares. La visualización se puede modificar de varias maneras, lo que proporciona información o aspectos adicionales sobre los datos. La visión de datos se puede ver con cascos de realidad virtual.

La visión de datos es una respuesta a este paradigma que cambia constantemente. Añade la flexibilidad de la percepción visual humana para detectar asociaciones y movimientos en los datos, independientemente del tipo de ataque, que de lo contrario pasarían desapercibidos.

La visión de datos convierte datos auditados en una visualización cronológica en 3-D de los orígenes y destinos de datos, mostrando como se van realizando las transacciones exactamente tal como se producen. El espacio de visualización contiene dos planos, cada uno representa entidades del dominio de auditoría de un tipo. Cada entrada de los datos de auditoría se representa como una 'línea parpadeante' que se mueve desde un objeto del plano superior (dirección IP de cliente, usuario de SO, usuario de base de datos, programa fuente) a un objeto en el plano inferior (base de datos, objeto o servidor). La línea parpadeante entre el origen y el destino deja un camino (una línea punteada) que indica la presencia de la interacción entre el origen y el destino específicos, que gradualmente se desvanece en el fondo. La línea parpadeante tiene el mismo color que la base de datos de destino. Los caminos proporcionan una visión general de la interacción entre los orígenes y los destinos en el periodo de tiempo seleccionado. Los orígenes están ubicados cerca de sus destinos y cerca de otros orígenes similares. El tamaño de la entidad de destino es proporcional al volumen de transacciones en relación con las otras entidades de destino. Hay muchas formas de modificar la visualización, entre otras por: el código de color de la entidad superior (cambios de color a medida que cambian los detalles del origen de datos), el filtro desde el gráfico de la visión de datos y las facetas de panel de control de investigación. La visión de datos también se puede ver con cascos de realidad virtual.

Procedimiento

1. En la ventana Panel de control de investigación, pulse Añadir gráfico > Gráfico de visión de datos. Se abre la ventana Valores de gráfico.
2. En el panel Valores de gráfico, modifique los tipos de objeto representados en los dos planos, el tipo de flujo de datos entre ellos. Si lo desea, puede ordenar por colores las entidades en el plano superior mediante un criterio secundario, proporcionando otro nivel de análisis. Por ejemplo, si los objetos del plano superior representan IP de cliente y selecciona la clasificación por colores para el programa fuente, puede ver el uso de distintos programas fuente según un cliente de IP específico, y el uso de un programa fuente común según las IP de cliente diferentes. Un objeto cuyo color cambia repetidamente indica un cambio frecuente del uso del programa fuente en una IP de cliente individual. Pulse Aplicar.

Tabla 1. Valores de gráfico de visión de datos

Campo	Descripción y valores

Campo	Descripción y valores
Dominio del flujo de datos	El tipo de flujo de datos visualizado. Uno de los siguientes: Actividades, Errores, Infracciones, Valores atípicos.
Entidades del plano superior	La entidad que se representa en el plano superior. Una de los siguientes: IP de cliente, Usuario de BD, Usuario de SO, Programa fuente.
Entidades del plano inferior	La entidad que se representa en el plano inferior. Una de las siguientes: Base de datos, Objeto, Servidor.
Clasificar por colores las entidades superiores por	Clasificación por colores adicional (opcional) de las entidades superiores por: Ninguno, IP de cliente, Usuario de BD, Usuario de SO, Programa fuente.
Mostrar etiquetas del plano superior	sí, no
Mostrar etiquetas del plano inferior	sí, no
Máx. de entidades en el plano superior	Número máximo de entidades que se muestran en el plano superior.
Máx. de entidades en el plano inferior	Número máximo de entidades que se muestran en el plano inferior.
Color de las entidades superiores	Abre la paleta de colores para seleccionar el color para las entidades de plano superior. Inhabilitado si las entidades superiores están clasificadas por colores.
Color de fondo	Abre una paleta de colores para seleccionar el color para el fondo.
Color de planos	Abre una paleta de colores para seleccionar el color de los planos (un color para ambos planos).

3. Modifique la visualización haciendo lo siguiente:
   - Pulse el icono de lupa para entrar en la modalidad de pantalla completa para obtener más detalles
   - Rote la vista manteniendo pulsado el botón izquierdo del ratón y arrastrando
   - Obtenga una panorámica manteniendo pulsado el botón derecho del ratón y arrastrando
   - Para aumentar y reducir, utilice la rueda del ratón
4. Vea entidades haciendo lo siguiente:
   - Pase el puntero del ratón sobre una entidad para ver sus detalles en la leyenda.
   - Pulse una entidad para ver solo sus flujos de datos (las otras entidades desaparecen progresivamente). Pulse el fondo para salir.
   - Realice una doble pulsación sobre una entidad para utilizarla como filtro activo (en todo el panel de control).
5. El panel de información, que se encuentra en la esquina superior derecha, muestra la indicación de fecha y hora de las acciones visualizadas actuales, el número de acciones que se muestran hasta el momento y una indicación de la tasa de sucesos por segundo. El usuario puede modificar la visualización haciendo lo siguiente:

	Poner en pausa/reiniciar flujo de datos
	Reiniciar flujo de datos desde el comienzo del periodo de tiempo
	Aumentar la velocidad del flujo de datos
	Reducir la velocidad del flujo de datos
	Ver desde parte superior (vista de pájaro)
	Ver desde parte lateral (valor predeterminado)

6. Utilice estos botones situados encima del Panel de control como corresponda:

	Activa la modalidad de pantalla completa para el gráfico de visión de datos
	Abre los valores de gráfico
	Cierra el gráfico de visión de datos
	Abre una ayuda emergente

Tema principal: Panel de control de investigación

Detección de valores atípicos

Habilite e inicie la auditoría de detección de valores atípicos en dos pasos sencillos, permitiendo que Guardium haga el trabajo de identificar el comportamiento anormal del usuario y del servidor, y proporcionando una detección temprana de posibles ataques.

Un valor atípico es el resultado de un comportamiento de un origen concreto (en DAM una base de datos o un usuario concreto en una base de datos, y desde Guardium V.10.1.2 en FAM en un servidor o en un usuario del sistema operativo), en un ámbito o periodo de tiempo concreto que está fuera del ámbito o marco temporal "normal" de la actividad del usuario o la base de datos concreta. Los valores atípicos pueden indicar una infracción de seguridad que está teniendo lugar, incluso si las propias actividades no infringen directamente una política de seguridad existente.

La actividad de usuario que se identifica como valor atípico sospechoso incluye:

- Un usuario que accede a una tabla por primera vez
- Un usuario que selecciona datos específicos en una tabla que él nunca ha seleccionado antes
- Un volumen excepcional de errores. Por ejemplo, una aplicación genera más errores de SQL de los que tiene en el pasado. Esto podría indicar que hay un ataque por inyección SQL en curso.
- Una actividad que por sí misma no es inusual, pero su volumen es inusual
- Una actividad que por sí misma no es inusual, pero el tiempo de la actividad es inusual. Por ejemplo, un DBA está accediendo a una tabla determinada con más frecuencia que en el pasado. Esto podría indicar que el DBA está descargando lentamente las pequeñas cantidades de datos a lo largo del tiempo.

La actividad de base de datos que se identifica como un valor atípico sospechoso incluye:

- Un volumen de errores excepcional

- Una actividad que por sí misma no es inusual, pero su volumen es inusual
- Una actividad que por sí misma no es inusual, pero el tiempo de la actividad es inusual

Los resultados de valores atípicos están disponibles en el Panel de control de investigación (Búsqueda rápida) y en los informes.

La minería de valores atípicos opera sobre datos que ya se han auditado mediante una política de seguridad. Asegúrese de que los datos que desea evaluar para los valores atípicos ya se han auditado mediante una política de seguridad.

La detección de valores atípicos se puede ejecutar en:

- Un agregador, con datos de todos sus recopiladores (excepto un recopilador que está ejecutando localmente la detección de valores atípicos).
- Un recopilador que utiliza datos, sólo sus propios datos.

- Inicio rápido para la detección de valores atípicos
  Aprenda a habilitar los valores atípicos y empiece a recibir alertas en unos pasos sencillos.
- Habilitación e inhabilitación de la detección de valores atípicos en un agregador
  Habilite, inhabilite y configure la detección de valores atípicos en agregados para configurar la detección de valores atípicos en todos los recopiladores del agregador.
- Habilitación e inhabilitación de la detección de valores atípicos localmente en un recopilador
  Ejecute la detección de valores atípicos en un único recopilador para evaluar únicamente los datos de ese recopilador.
- Interpretación de valores atípicos de datos en el panel de control de investigación
  Guardium proporciona una práctica interfaz gráfica para identificar y responder a los valores atípicos detectados por el algoritmo.
- Interpretación de los valores atípicos de actividad de archivos
  Visualice los valores atípicos de supervisión de actividad en el Gráfico de actividades del panel de control de investigación y en la Tabla de resultados (el panel de control debe estar habilitado) o revise el informe Lista de valores atípicos de analítica.
- Supervisar el estado de minería de valores atípicos
  Utilice la página de estado de minería de valores atípicos para supervisar el proceso de minería de valores atípicos tanto en una unidad específica donde se ejecuta el proceso como en un agregador o Gestor central (CM).
- Agrupación de usuarios y objetos para la detección de valores atípicos
  Obtenga información sobre cómo añadir grupos, por ejemplo grupos de usuarios o u objetos, al algoritmo predeterminado de detección de valores atípicos.
- Exclusión de sucesos de la detección de valores atípicos
  Es posible excluir sucesos de la detección de valores atípicos, por ejemplo, la actividad de los datos de prueba.

Tema principal: Supervisar y auditar

Inicio rápido para la detección de valores atípicos

Aprenda a habilitar los valores atípicos y empiece a recibir alertas en unos pasos sencillos.

Antes de empezar

- La detección de anomalías está habilitada (Configuración > Herramientas y vistas > Detección de anomalías).

Acerca de esta tarea

La detección de valores atípicos se puede ejecutar en cualquier número de agregadores. Sin embargo, se recomienda empezar con un agregador, refinar la configuración y, a continuación, ampliar a más agregadores. Antes de empezar, debe definir la investigación de valores atípicos de acuerdo a los recursos disponibles. A continuación debe limitar el número de valores atípicos informados diariamente a una cantidad que pueda investigar. El algoritmo de guardium proporciona los sucesos más importantes que es necesario investigar y no tan solo los primeros 10 más importantes, por ejemplo.

La detección de valores atípicos es un proceso independiente de los procesos de obligatoriedad y de las reglas de política de seguridad, de forma que no es posible configurar alertas en tiempo real con los valores atípicos. Sin embargo, puesto que los datos de los valores atípicos se incluyen en los informes, puede crear una alerta de correlación. Una alerta de correlación la desencadena una consulta que mira hacia atrás en un periodo de tiempo especificado para determinar si se ha alcanzado un umbral de alerta.

Procedimiento

1. Habilite valores atípicos; consulte Habilitación e inhabilitación de la detección de valores atípicos en un agregador o Habilitación e inhabilitación de la detección de valores atípicos localmente en un recopilador.
2.
3. Establezca el número máximo de valores atípicos de los que quiere ser informado cada día. Consulte .
4. Opcionalmente, realice un ajuste fino de la definición del valor atípico. Consulte Agrupación de usuarios y objetos para la detección de valores atípicos y Exclusión de sucesos de la detección de valores atípicos.
5. Cree una consulta.
   a. Vaya a Informes > Herramientas de configuración de informes > Creador de consultas.
   b. Establezca Dominio=analítico, Nombre de consulta=Lista de valores atípicos de analítica o Resumen de valores atípicos de analítica por fecha. Los demás valores se pueden dejar en sus valores predeterminados.
   c. Pulse Crear informe.
6. Cree un proceso de auditoría.
   a. Vaya a Cumplir > Herramientas y vistas > Creador de procesos de auditoría.
   b. Asigne un nombre al proceso y añada la tarea (el informe que acaba de crear).
   c. Defina receptores. Decida qué tipo de notificaciones desea. Puede establecer alertas, añadir a la lista de tareas pendientes y asignar usuarios para revisar y justificar las conclusiones.
   d. Planifique el proceso como diario y pulse Guardar.
7. Para una visualización fácil, añada los informes de los valores atípicos a Mi panel de control.

Resultados

Cuando se completa el periodo de aprendizaje después de una semana, debería haber datos en los informes, y se deberían enviar alertas.
Tema principal: Detección de valores atípicos

Habilitación e inhabilitación de la detección de valores atípicos en un agregador

Habilite, inhabilite y configure la detección de valores atípicos en agregados para configurar la detección de valores atípicos en todos los recopiladores del agregador.

Antes de empezar

- Se recomienda encarecidamente que habilite los valores atípicos sólo en los agregadores de 64 bits con un mínimo de 24 gigabytes de memoria.

Esta característica recibe soporte de Guardium V.10.1.2.

Acerca de esta tarea

Restricción: La detección de valores atípicos y la seguridad a nivel de datos no se pueden habilitar de forma simultánea.

Cuando se ejecuta en el agregador, se extraen datos de detección de valores atípicos desde las unidades gestionadas y las fases de aprendizaje y análisis se realizan en el agregador.

La detección de valores atípicos está inhabilitada de forma predeterminada. Este procedimiento se ejecuta en un gestor central, para habilitar o inhabilitar la detección de valores atípicos en todos los recopiladores que envían sus datos al agregador especificado, excepto un recopilador que está ejecutando localmente la detección de valores atípicos. (Para obtener más detalles sobre la recopilación local, consulte Habilitación e inhabilitación de la detección de valores atípicos localmente en un recopilador).

Si un recopilador se ha movido de un agregador a otro, o si desea habilitar la detección de valores atípicos localmente en un recopilador, inhabilite la detección de valores atípicos en el agregador, habilite la detección de valores atípicos localmente si es pertinente y, a continuación, habilite la detección de valores atípicos en el agregador. Siempre que habilite la detección de valores atípicos en el agregador, se renueva la lista de sus recopiladores.

Procedimiento

1. Inicie la sesión en el gestor central como un usuario o administrador con el rol de CLI.
2. Para habilitar la función de detección de valores atípicos, entre:

   ```
   grdapi enable_outliers_detection_agg schedule_interval=1 schedule_units=HOUR aggregator_host_name=<aggregator host name>
   DAM_FAM=DAM
   ```

   donde:

   - el parámetro aggregator_host_name es el nombre de host del agregador
   - FAM_DAM es un parámetro opcional que especifica el tipo de valores atípicos. El valor predeterminado es DAM.

3. Para inhabilitar la función de detección de valores atípicos, especifique:

   ```
   grdapi disable_outliers_detection_agg aggregator_host_name=<aggregator host name>
   ```

   donde:

   - el parámetro aggregator_host_name es el nombre de dominio completo del agregador

Resultados

El sistema empieza a recopilar datos atípicos. Una vez que el aprendizaje se ha completado (14 días), los datos atípicos están disponibles en el panel de control de investigación (Interpretación de valores atípicos de datos en el panel de control de investigación y Interpretación de los valores atípicos de actividad de archivos) y en el informe de lista analítica de valores atípicos.

Tema principal: Detección de valores atípicos
Conceptos relacionados:
Panel de control de investigación
Información relacionada:
Funciones de detección de valores atípicos de GuardAPI

Habilitación e inhabilitación de la detección de valores atípicos localmente en un recopilador

Ejecute la detección de valores atípicos en un único recopilador para evaluar únicamente los datos de ese recopilador.

Antes de empezar

- Se recomienda encarecidamente que habilite los valores atípicos sólo en los recopiladores de 64 bits con un mínimo de 24 gigabytes de memoria.

Acerca de esta tarea

Restricción: La detección de valores atípicos y la seguridad a nivel de datos no se pueden habilitar de forma simultánea.

La detección de valores atípicos está inhabilitada de forma predeterminada. Siga los pasos que se describen a continuación para habilitar o inhabilitar la detección de valores atípicos localmente en un recopilador. Cuando la detección de valores atípicos está habilitada localmente en un recopilador, sus datos no se combinan con los datos de su agregador.

Para identificar un recopilador que esté ejecutando la minería de valores atípicos a nivel local, acceda a la ventana de estado de minería de valores atípicos y mire la fila del recopilador individual (no bajo el agregador). La columna Minería de valores atípicos habilitada/inhabilitada se muestra en verde.

Para cambiar una detección de valores atípicos entre el local y el agregador, inhabilite la detección de valores atípicos localmente, inhabilite la recopilación de valores atípicos en el agregador y renueve la lista de recopiladores volviendo a habilitar la detección de valores atípicos en el agregador.

Procedimiento

1. Inicie la sesión en el recopilador como usuario o administrador con el rol de CLI.
2. Para habilitar la función de detección de valores atípicos, entre:

   ```
   grdapi enable_outliers_detection schedule_interval=1 schedule_units=HOUR DAM_FAM=DAM
   ```

   donde:

   - FAM_DAM es un parámetro opcional que especifica el tipo de valores atípicos. El valor predeterminado es DAM.

3. Para inhabilitar la función de detección de valores atípicos, especifique:

   ```
   grdapi disable_outliers_detection
   ```

Resultados

El sistema empieza a recopilar datos atípicos. Una vez que el aprendizaje se ha completado (7 días), los datos atípicos están disponibles en el panel de control de investigación (consulte Interpretación de valores atípicos de datos en el panel de control de investigación y Interpretación de los valores atípicos de actividad de archivos) y el informe de lista analítica de valores atípicos.

Tema principal: Detección de valores atípicos
Información relacionada:
Funciones de detección de valores atípicos de GuardAPI

Interpretación de valores atípicos de datos en el panel de control de investigación

Guardium proporciona una práctica interfaz gráfica para identificar y responder a los valores atípicos detectados por el algoritmo.

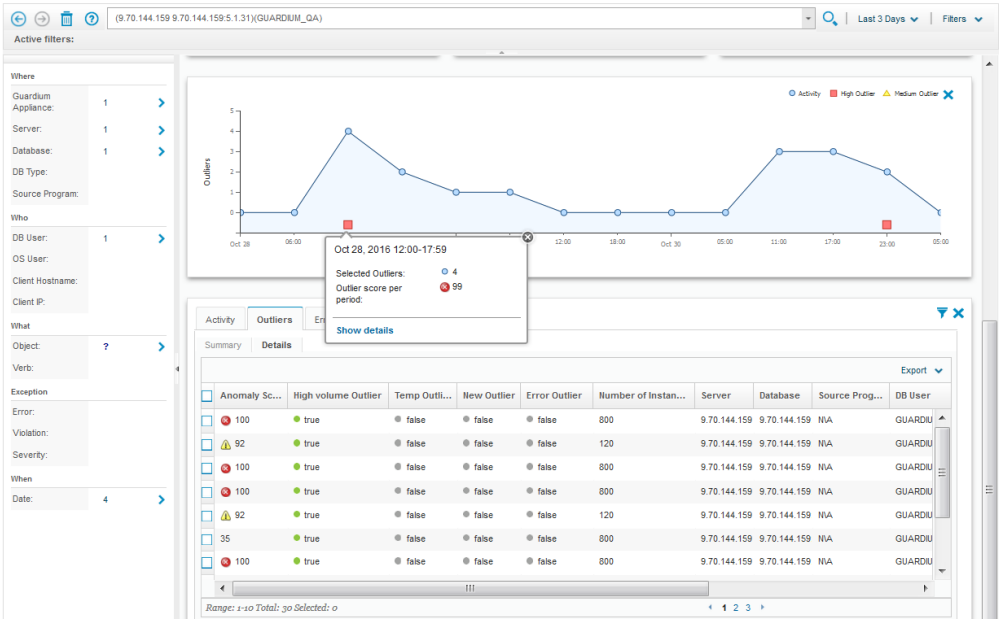
La búsqueda rápida debe estar habilitada (grdapi enable_quick_search) para ver datos de detección de valores atípicos en el panel de control de investigación.

El Gráfico de actividades incluye indicadores rojos (alto) y amarillo (medio) que reflejan la gravedad o la puntuación total de valores atípicos para el intervalo de tiempo seleccionado. Los indicadores rojos reflejan los sucesos altamente anómalos que requieren una atención inmediata. Los indicadores amarillos representan anomalías menos radicales que justifican la atención como parte de otras investigaciones o investigaciones relacionadas.

Pase el puntero del ratón sobre un icono de valor atípico para ver información detallada sobre los valores atípicos detectados durante ese periodo de tiempo. Para filtrar la tabla de resultados para actividades o valores atípicos que se han producido durante el mismo periodo de tiempo, pulse Mostrar detalles.

A partir de Guardium V.10.1.2, el separador Valores atípicos de la tabla de resultados tiene dos vistas:

- El resumen tiene una fila por origen por hora en la que se ha encontrado un valor atípico, con una puntuación de anomalía y una o más razones. Tenga en cuenta que no todos los valores atípicos que se presentan en el separador Resumen tienen más detalles en el separador Detalles.
- Los detalles son un ejemplo de sucesos que se han producido, con una fila por suceso con una razón (excepto diverso, consulte la tabla) y otros detalles (programa fuente, objeto, verbo, etc.) . Por ejemplo, para un volumen alto, el muestreo presenta los sucesos con la puntuación más alta. Puede configurar el número de ejemplos (filas) que aparecen en el separador Detalles, por cada valor atípico en el separador Resumen.



Esta tabla describe las columnas de las vistas Resumen y Detalles:

Tabla 1. Columnas en los separadores de valores atípicos de la tabla de resultados

Nombre de columna	Descripción	Acción adicional

Nombre de columna	Descripción	Acción adicional
Puntuación de anomalía	Separador Resumen: Un valor agregado calculado basado en el volumen de valores atípicos, la gravedad de sucesos individuales, el volumen previsto de valores atípicos para una determinada una hora del día y otros factores. Por ejemplo, en un sistema que normalmente identifica 0 valores atípicos a la 01:00 y 5-10 valores atípicos a las 13:00 durante los días laborables, la presencia de dos valores atípicos adicionales (de 2 valores atípicos a la 01:00 o de 12 valores atípicos a las 13:00) es más significativa, y se pondera más, que el total por horas. Separadores Detalles: La puntuación de anomalía solo es relevante para un suceso de alto volumen.	Pulse con el botón derecho del ratón en la puntuación para abrir un menú con acciones adicionales que puede realizar. En el separador Detalles, la puntuación puede ser 0, lo que indica que los sucesos individuales no son sospechosos por sí mismos, aunque los sucesos acumulados en esa hora son sospechosos.
Valor atípico de alto volumen	Verdadero o falso. Alto volumen de actividades de algún tipo, por ejemplo sobre un objeto, de un usuario de base de datos.	
Nuevo valor atípico	Verdadero o falso. Alto volumen de actividades en objetos nuevos, por ejemplo, un administrador crea de manera inusual un gran número de tablas nuevas.	
Valor atípico diverso	Solo vista de resumen. Verdadero o falso. Alto volumen de distintos tipos de actividades, por ejemplo, un usuario de la base de datos realiza muchas más actividades de las habituales, o las realiza en un momento inusual. Un ejemplo de sucesos diversos no aparece en el separador Detalles, pueden ser identificados por el usuario de la base de datos. Aunque Diverso no es una columna en el separador de detalles, es posible que tengan otras razones asignadas. De lo contrario aparecen sin una razón.	Consulte la tabla Actividad para obtener más detalles.
Valor atípico de error	Verdadero o falso. Alto volumen de errores	
Valor atípico en curso	Solo vista de resumen. Verdadero o falso. Suceso en las últimas horas que no fue lo suficientemente alto como para crear un valor atípico, aunque sí levantar sospechas.	No hay ningún suceso específico para ver. Consulte la tabla Actividad, filtre por la base de datos en la lista de facetas y modifique el intervalo de tiempo hasta el momento del comportamiento sospechoso.
Número de instancias	Solo vista de detalles. Número de veces que se ha visto este suceso concreto en la hora	
Registros afectados	Número de registros afectados por la solicitud concreta. Aparece como un número negativo si el suceso no tiene, por definición, registros afectados.	
Servidor	Servidor en el que se ha producido el suceso	
Base de datos	Base de datos en la que se ha producido el suceso	
Programa fuente	Solo vista de detalles. El programa fuente en la que se ha producido el suceso	
Usuario de BD	Solo vista de detalles. El usuario de BD que ha ejecutado el suceso de valor atípico.	
Objeto	Objeto en el que el usuario ha ejecutado el suceso	
Usuario privilegiado	Solo vista de resumen. Verdadero o falso. Si el usuario tiene o no tiene privilegios	
Verbo	Solo vista de detalles. Verbo en el que el usuario ha ejecutado el suceso	
Fecha	Fecha en la que se ha producido el suceso en el formato aaaa-mm-dd	
Hora	Hora en la que se ha producido el suceso en el formato hh:mm:ss	

Antes de Guardium V.10.1.2, existía una columna de razón de valor atípico, con uno o varios de estos valores:

Inusual
: una condición rara vez vista

Alto volumen
: una incidencia inusualmente alta de una condición

Nuevo
: una condición vista por primera vez

Error
: una incidencia inusualmente alta de condiciones de error

Las razones de valores atípicos se asignan en combinaciones cuando es necesario. Por ejemplo, un valor atípico se puede marcar como un volumen inusual y alto si una condición rara vez vista de repente se produce muchas veces.

Nota:

Si aparece un resultado negativo ("-") en el informe de resultados de Registros afectados, el usuario debe volver a habilitar los valores atípicos para borrar este resultado negativo.

Tema principal: Detección de valores atípicos
Información relacionada:
Detección de anomalías

Interpretación de los valores atípicos de actividad de archivos

Visualice los valores atípicos de supervisión de actividad en el Gráfico de actividades del panel de control de investigación y en la Tabla de resultados (el panel de control debe estar habilitado) o revise el informe Lista de valores atípicos de analítica.

Los valores atípicos dan soporte a la supervisión de actividad de archivos a partir de Guardium V.10.1.2

La búsqueda rápida debe estar habilitada (grdapi enable_quick_search) para ver datos de detección de valores atípicos en el panel de control de investigación.

Visualice los valores atípicos en el Gráfico de actividades del panel de control de investigación y en la Tabla de resultados (el panel de control debe estar habilitado) o revise el informe Lista de valores atípicos de analítica.

Acceda al gráfico de resumen seleccionando Datos o desde el menú desplegable Interfaz de usuario y pulsando Intro; o bien especificando una búsqueda rápida en el campo de búsqueda y pulsando Intro.

El Gráfico de actividades incluye indicadores rojos (alto) y amarillo (medio) que reflejan la gravedad o la puntuación total de valores atípicos para el intervalo de tiempo seleccionado. Los indicadores rojos reflejan los sucesos altamente anómalos que requieren una atención inmediata. Los indicadores amarillos representan anomalías menos radicales que justifican la atención como parte de otras investigaciones o investigaciones relacionadas.

Pase el puntero del ratón sobre un icono de valor atípico para ver información detallada sobre los valores atípicos detectados durante ese periodo de tiempo. Para filtrar la tabla de resultados por actividades o valores atípicos que se han producido durante el mismo periodo de tiempo, pulse Mostrar detalles.

El separador Valores atípicos de la tabla de resultados tiene dos vistas:

- El resumen tiene una fila por origen por hora en la que se ha encontrado un valor atípico, con una puntuación de anomalía y una o más razones. Tenga en cuenta que no todos los valores atípicos que se presentan en el separador Resumen tienen más detalles en el separador Detalles.
- Los detalles son un ejemplo de sucesos que se han producido, con una fila por suceso con una razón y otros detalles. Por ejemplo, para un volumen alto, el muestreo presenta los sucesos con la puntuación más alta. Puede configurar el número de ejemplos (filas) que aparecen en el separador Detalles, por cada valor atípico en el separador Resumen.

Esta tabla describe las columnas de las vistas Resumen y Detalles:

Tabla 1. Columnas definidas para Resumen y Detalles

Nombre de columna	Descripción	Acción adicional
Puntuación de anomalía	Separador Resumen: Un valor agregado calculado basado en el volumen de valores atípicos, la gravedad de sucesos individuales, el volumen previsto de valores atípicos para una determinada una hora del día y otros factores. Por ejemplo, en un sistema que normalmente identifica 0 valores atípicos a la 01:00 y 5-10 valores atípicos a las 13:00 durante los días laborables, la presencia de dos valores atípicos adicionales (de 2 valores atípicos a la 01:00 o de 12 valores atípicos a las 13:00) es más significativa, y se pondera más, que el total por horas. Separadores Detalles: La puntuación de anomalía solo es relevante para un suceso de alto volumen.	Pulse con el botón derecho del ratón en la puntuación para abrir un menú con acciones adicionales que puede realizar. En el separador Detalles, la puntuación puede ser 0, lo que indica que los sucesos individuales no son sospechosos por sí mismos, aunque los sucesos acumulados en esa hora son sospechosos.
Valor atípico de alto volumen	Verdadero o falso. Alto volumen de actividades de algún tipo, por ejemplo sobre un objeto, de un usuario de base de datos.	
Nuevo valor atípico	Verdadero o falso. Alto volumen de actividades en objetos nuevos, por ejemplo, un administrador crea de manera inusual un gran número de tablas nuevas.	
Valor atípico de error	Verdadero o falso. Alto volumen de errores	
Valor atípico en curso	Solo vista de resumen. Verdadero o falso. Suceso en las últimas horas que no fue lo suficientemente alto como para crear un valor atípico, aunque sí levantar sospechas.	No hay ningún suceso específico para ver. Consulte la tabla Actividad, filtre por la base de datos en la lista de facetas en el momento del comportamiento sospechoso.
Número de instancias	Solo vista de detalles. Número de veces que se ha visto este suceso concreto en la hora	
Servidor	Servidor en el que se ha producido el suceso	
Usuario de SO	Usuario de SO que ha ejecutado el suceso	
Usuario privilegiado	Verdadero o falso. Si el usuario tiene o no tiene privilegios	
Nombre de archivo completo	Nombre del archivo en el que el usuario ha ejecutado el suceso	
Mandato	Mandato con el que el usuario ha ejecutado el suceso	
Fecha	Fecha en la que se ha producido el suceso en el formato aaaa-mm-dd	
Hora	Hora en la que se ha producido el suceso en el formato hh:mm:ss	

Tema principal: Detección de valores atípicos
Conceptos relacionados:
Panel de control de investigación
Información relacionada:
Funciones de detección de valores atípicos de GuardAPI
Detección de anomalías

Supervisar el estado de minería de valores atípicos

Utilice la página de estado de minería de valores atípicos para supervisar el proceso de minería de valores atípicos tanto en una unidad específica donde se ejecuta el proceso como en un agregador o Gestor central (CM).

La página de estado de minería de valores atípicos que se visualiza en el Gestor central presenta detalles de todos los agregadores gestionados y sus recopiladores. Todos los recopiladores en el Gestor central aparecen en filas individuales bajo sus agregadores. Cuando se visualiza en un agregador, esta ventana presenta detalles de los recopiladores del agregador específico. Cuando se visualiza desde un recopilador, solo se presenta un solo recopilador.

La página se encuentra en el menú de Guardium Gestionar > Mantenimiento > Estado de minería de valores atípicos.

Las tablas siguientes describen la página y las acciones de usuario recomendadas.

Tabla 1. Columnas de la página de estado de minería de valores atípicos

Columna	Descripción	Acciones
Unidad	Nombre de la unidad	N/D
	Abre la lista de unidades que envían datos a este agregador	Pulse aquí para ver la lista de unidades
Unidad activada/desactivada	Indica si la unidad está activada o desactivada.	N/D
Minería de valores atípicos habilitada/inhabilitada	• Agregador: Indica si está habilitada la minería de valores atípicos en el agregador. Si está inhabilitada, el resto de la fila después de esta columna está vacía. • Fila individual de un recopilador o una unidad autónoma: Verde indica que la minería de valores atípicos está habilitada localmente.	N/D
Enviar datos para minería de valores atípicos	Solo recopiladores. El recopilador envía datos de minería de valores atípicos al agregador. Los datos para la minería de valores atípicos se envían desde el recopilador al agregador si el agregador está habilitado para la minería de valores atípicos y el recopilador no está ejecutando localmente valores atípicos en la minería.	N/D
Última anomalía encontrada	Fecha y hora local en el Gestor central del último proceso de minería de valores atípicos que ha encontrado una o más anomalías (valores atípicos). Muestra datos solo para las unidades que ejecutan la versión 10.1.2 y posteriores.	N/D
Último análisis	Fecha y hora local en el Gestor central del último proceso de minería de valores atípicos (fecha/hora de finalización de proceso). Muestra datos solo para las unidades que ejecutan la versión 10.1.2 y posteriores.	N/D
Estado de minería de valores atípicos	El estado del último proceso de minería de valores atípicos. Verde: El proceso ha finalizado satisfactoriamente. Amarillo: El proceso ha finalizado con avisos. Rojo: El proceso ha finalizado con errores. Muestra datos solo para las unidades que ejecutan la versión 10.1.2 y posteriores.	Si se ha producido un error/aviso solo una vez, deje que el proceso se ejecute de nuevo (hora siguiente) y compruebe el resultado. Si se repite un error, póngase en contacto con el servicio de soporte.
Detalles	El estado puede ser rojo (error), amarillo (aviso) o verde.	Para los procesos que han finalizado con avisos (amarillo), pulse para abrir una ventana emergente con el aviso. Para los procesos que han finalizado con errores (rojo), pulse para abrir una ventana emergente con el error.
Aprendizaje desde	Fecha y hora en la que se habilitó el proceso de minería de valores atípicos. El proceso conoce el comportamiento del recurso a partir de esta hora.	N/D
Búsqueda rápida activada/desactivada	Indica si la Búsqueda rápida y Solr están habilitados en la unidad gestionada. Cuando la búsqueda rápida está inhabilitada, los datos de esta máquina no se incluyen en el panel de control de investigación.	Consulte Habilitación e inhabilitación del panel de control de investigación
Última actualización de información	Última fecha y hora en que se actualizó la información de esta fila. Los datos se suelen actualizar en intervalos de 5 minutos.	N/D

Tabla 2. Botones de la página de estado de minería de valores atípicos

Botón	Descripción	Acciones
Renovar	Renueva la pantalla	Pulse para renovar la pantalla
Signo más	Este botón aparece solo cuando la unidad detallada en la fila es un agregador.	Pulse aquí para abrir la lista de unidades que envían datos a este agregador.

Tema principal: Detección de valores atípicos

Agrupación de usuarios y objetos para la detección de valores atípicos

Obtenga información sobre cómo añadir grupos, por ejemplo grupos de usuarios o u objetos, al algoritmo predeterminado de detección de valores atípicos.

Acerca de esta tarea

De forma predeterminada, hay dos grupos de usuarios y objetos que se ponderan o puntúan más por el algoritmo de aprendizaje de máquina de Guardium: los usuarios administrativos y los objetos confidenciales. Sin embargo, es posible que ya haya establecido grupos adicionales que también resultarían útiles para la detección de

valores atípicos. Por ejemplo, es posible que tenga un grupo de usuarios sospechosos o que tenga varios grupos de objetos confidenciales que estén alineados con distintas aplicaciones.

Procedimiento

1. Esta tarea requiere que conozca el ID de grupo interno que se va a utilizar con el mandato grdapi. Para obtener el ID de grupo, puede utilizar el siguiente mandato: `grdapi list_group_by_desc desc=[group name]`. Por ejemplo, si tiene un grupo denominado BadGuys, puede especificar el siguiente mandato para obtener su ID de grupo interno:

   ```
   grdapi list_group_by_desc desc="BadGuys"
   ```

2. Una vez que sepa el ID deseado, añádalo como un grupo de usuarios privilegiado para una mejora en la puntuación tal como se indica (observe que también debe incluir el grupo predeterminado 1 si también desea mejorar las puntuaciones para el mismo). Para añadir un grupo con el ID 1234: grdapi set_outliers_detection_parameter parameter_name="privUsersGroupIds" parameter_value=1,1234
3. Para añadir objetos sensibles con los ID 333 y 156: set_outliers_detection_parameter parameter_name="sensitiveObjectGroupIds" parameter_value=5,333,156

Resultados

Los grupos especificados o los objetos confidenciales se añaden a la detección de valores atípicos y el algoritmo les otorga ponderación adicional.

Tema principal: Detección de valores atípicos

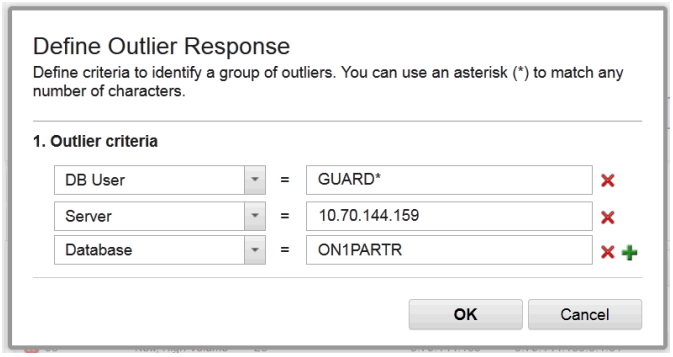
Exclusión de sucesos de la detección de valores atípicos

Es posible excluir sucesos de la detección de valores atípicos, por ejemplo, la actividad de los datos de prueba.

Excluir sucesos que coincidan con criterios específicos, utilizando la respuesta ante el valor atípico

1. Pulse con el botón derecho del ratón en un indicador de valores atípicos y seleccione Ignorar para excluir las respuestas ante el valor atípico.
2. Especifique valores específicos o utilice entradas de caracteres comodín (con el carácter *) para definir lo que desea ignorar.
3. Elimine todos los campos que no sean necesarios pulsando los iconos ✖ correspondientes.
4. Pulse Aceptar para confirmar los cambios.
5. Para incluir sucesos ignorados anteriormente, vea el informe Comentarios de los usuarios de analítica, efectúe una doble pulsación en el suceso que se ha ignorado anteriormente y seleccione Invocar > delete_analytic_user_feedback.

Por ejemplo, para ignorar toda la actividad del servidor 10.70.144.159, base de datos ON1PARTR y cualquier usuario de base de datos que empiece por GUARD, el diálogo se parece a:

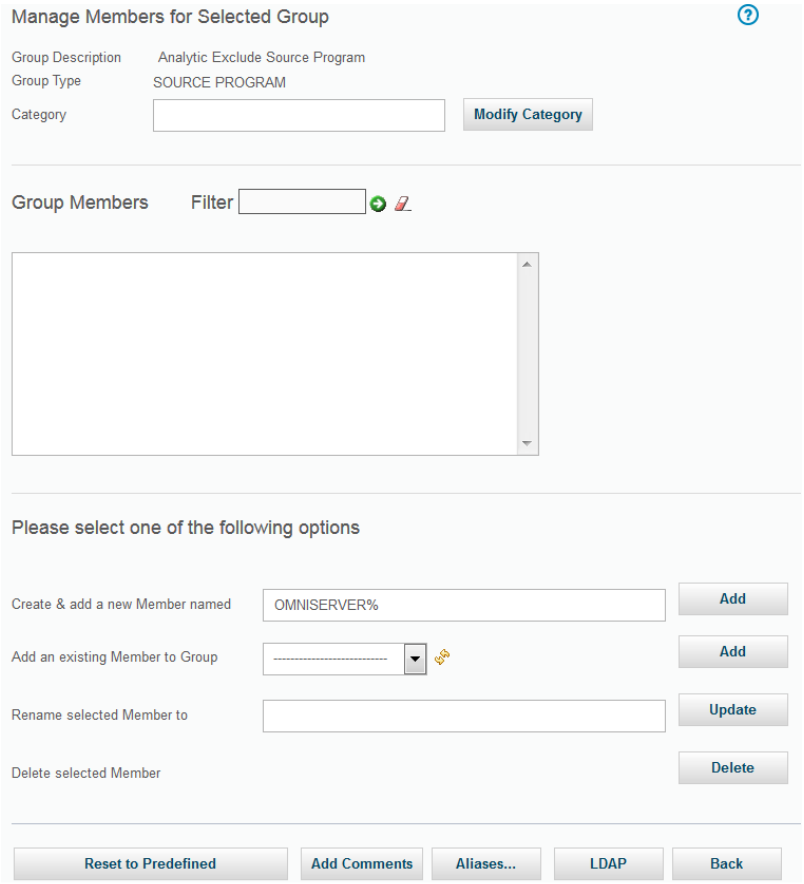


Excluir sucesos utilizando el Creador de grupos

Si tiene muchos elementos para la exclusión, utilice el Creador de grupos de Guardium y rellene alguno o todos los grupos siguientes según sea necesario:

- Analytic Exclude DB User
- Analytic Exclude OS User
- Analytic Exclude Server IP
- Analytic Exclude Service Name
- Analytic Exclude Source Program

El Creador de grupos tiene opciones para la carga masiva incluida la capacidad de rellenar desde una consulta en una tabla personalizada.



De forma alternativa, utilice los mandatos de GuardAPI para rellenar los grupos Analytic Exclude. Por ejemplo, para añadir OMNISERVER al grupo Analytic Exclude Source Program, utilice el siguiente mandato:

```
grdapi create create_member_to_group_by_desc  desc="Analytic Exclude Source Program" member="OMNISERVER%"
```

Tema principal: Detección de valores atípicos

Panel de control de protección de datos

El panel de control de protección de datos de Guardium proporciona una vista de resumen de los datos de riesgo y cumplimiento destinados a los responsables de seguridad de nivel superior.

El panel de control de protección de datos contiene varios diagramas y gráficos, además de las estadísticas de riesgo y cumplimiento diseñadas para una visualización continua en un monitor grande. Para abrir el panel de control, vaya a Investigar > Panel de control de protección de datos Guardium.

PRECAUCIÓN:
La sesión no caducará y no se cerrará automáticamente la sesión mientras se visualiza el panel de control de protección de datos. Tenga cuidado cuando deja abierto el panel de control durante largos periodos de tiempo.
Información:

- El panel de control se renueva automáticamente cada 20 minutos.
- Los valores de búsqueda predeterminados son para la búsqueda distribuida con datos recopilados de un día anterior.

Gráficos y diagramas

Varios gráficos de líneas le permiten comparar rápidamente distintos tipos de datos. Por ejemplo, un gráfico puede mostrar el volumen de actividades, errores e infracciones a lo largo del tiempo.

Un gráfico de Actividades anómalas muestra un resumen de valores atípicos en relación con la actividad global. En este gráfico, un punto de resumen de valores atípicos representa un volumen inesperado de valores atípicos.

Información: El eje y de estos gráficos es un eje de registro y puede distorsionar las proporciones del gráfico, y los valores o recuentos no se registran.

Estadísticas de riesgo y cumplimiento

La estadística de Riesgo muestran el número de pruebas que han fallado con gravedad crítica y el número de orígenes de datos donde se han producido estos fallos. Cada origen de datos puede tener varias pruebas fallidas.

Orígenes de datos supervisados muestra el número de orígenes de datos para los que el sistema registra actividades. Esta estadística se calcula examinando los datos de dominio de acceso disponibles.

Tareas de la lista de tareas pendientes de conformidad muestra el siguiente resumen de procesos de auditoría: el número de procesos que se han cerrado hoy, el número de procesos que han estado abiertos durante menos de tres días y el número de procesos que han estado abiertos durante más de tres días.

Información:

- Las estadísticas no se ven afectadas por los filtros de búsqueda de texto y faceta, pero las estadísticas se ven afectadas por la modalidad de búsqueda. Para cambiar la modalidad de búsqueda, utilice el control para expandir el panel superior y luego pulse el icono para conmutar entre la búsqueda distribuida y local.
- Los componentes estadísticos se vuelven a calcular una vez cada hora.

Tema principal: Supervisar y auditar

Informes

Un informe define cómo se presentan los datos recopilados por una consulta.

El informe predeterminado es un informe tabular que refleja la estructura de la consulta, con cada atributo visualizado en una columna distinta. Todos los componentes de presentación de un informe tabular (por ejemplo, las cabeceras de columna) pueden personalizarse. Todos los informes gráficos se definen utilizando el Creador de informes. Además de los parámetros fecha de inicio y fecha de fin (fecha de consulta hasta y fecha de consulta desde), los valores ahora se pueden mostrar entre el principio de la página y el inicio de la tabla en todos los informes.

Antes de utilizar el Creador de informes, cree una consulta utilizando el Generador de consultas. Consulte Utilización del Creador de consultas.

La forma más rápida de crear y ver un informe es utilizando los pasos para crear un informe y, a continuación, seleccione el informe en Mi panel de control.

Mueva hacia adelante y atrás entre pantallas de menú utilizando los botones Anterior y Siguiente. La flecha atrás en el navegador web no funciona para la navegación entre pantallas Guardium.

Iconos utilizados en los Informes

Utilice los iconos para seleccionar funciones dentro de Creador de informes.

Tabla 1. Iconos de informe

Iconos gráficos	Función
	Proceso ad hoc para ejecutar una vez ahora
	Renovar
	Abrir o ejecutar en una nueva ventana
	Añadir un informe
	Añadir a Favoritos
	Modificar o editar la consulta para este informe o Personalizar gráfico
	Suprimir
	Constructor de despensa de datos
	Clonar
	Configurar parámetros de tiempo de ejecución
	Configurar columnas de informe
<-- --> <--	Personalizar informe

Buscar un informe para su edición

Para acceder a una definición de informes, seleccione el icono Informes de ciclo de vida y, a continuación, pulse Generador de informes.

Busque un informe eligiendo el título Dominio, Consulta o Informe. Los resultados se muestran en el panel Resultados de la búsqueda de informes.

- Para localizar un informe específico, seleccione dicho informe en la lista Título de informe. El informe seleccionado se visualiza inmediatamente en el panel Resultados de búsqueda de informes.

  Para los tipos de búsqueda restantes, pulse el botón Buscar después de realizar entradas en uno o más campos, o simplemente pulse el botón Buscar para listar todos los informes disponibles para su cuenta Guardium.

- Para listar todos los informes que utilizan una consulta específica, seleccione esa consulta en la lista Consultas.
- Para listar todos los informes para un tipo de diagrama específico, selecciónelo en la lista Tipo de diagrama.

Para localizar un informe específico, seleccione dicho informe en la lista Título de informe. El informe seleccionado se visualiza inmediatamente en el panel Resultados de búsqueda de informes.

Si la búsqueda localiza algún informe, se visualizan en el panel Resultados de la búsqueda de informes. Pulse en cualquiera de los botones siguientes:

- Nuevo: Consulte Crear un informe.
- Clonar: Consulte Clonar un informe.
- Modificar: Consulte Modificar un informe.
- Roles: Consulte Roles de seguridad. Asigne roles a los informes en el Creador de informes. La asignación de roles a informes mientras se está en Query Builder (Seguimiento) asigna sólo el rol a la consulta, no el informe.
- Suprimir: Consulte Eliminar un informe.
- Comentario: Consulte Comentarios.
- Asignación de API: Consulte Asignación de API
- Control profundizable: Consulte Modificar el menú Informes profundizables para un informe.

Crear un informe

1. Para acceder a una definición de informes, seleccione el icono Informes de ciclo de vida y, a continuación, pulse Creador de informes.
2. Pulse Nuevo para abrir el panel Crear informe.
3. En la lista Consulta, seleccione un valor de consulta para que lo utilice el informe (por ejemplo, Inicios de sesión de Guardium)
4. Especifique un nombre exclusivo para el informe en el campo Título del informe.

Personalización de la presentación de informe

Siga los procedimientos de pasos para personalizar la presentación del informe.

1. En el panel Descripciones de columna de informe.
   - Modifique opcionalmente el Título del informe. El valor predeterminado es de la definición de informe. Puede modificar el título en la mayoría de los paneles.
   - Opcionalmente, sustituya las descripciones de columna (las cabeceras de columna).
2. Pulse Siguiente para abrir el panel Atributos de informe:
   - Marque el botón Tabular o Gráfica.
   - Pulse Siguiente para ir al panel Enviar informe.
3. Pulse Guardar para enviar el informe para su creación.

Crear un informe gráfico

Siga los procedimientos de pasos para crear un informe gráfico.

1. Siga los pasos anteriores de Personalizar la presentación de informe para Descripciones de columna de informe, Descripciones de parámetros de informe y Atributos de informe.
2. En el panel Tipo de gráfico de informe, seleccione el tipo de gráfico y pulse Siguiente. Las opciones son Área, Barra, Área de barras, Línea de barras, Columna, Área de fechas, Columna de fecha, Línea de fecha, Línea de etiqueta distribuida, Barra individual, Columna individual, Línea, Pictograma, Circular, Polar, Velocímetro y Barra de pila. Se recomienda Circular, Polar, Velocímetro y Barra de pila. Elija una y pulse Siguiente.
3. Si el panel Tipo de gráfico de informe no se visualiza, omita este paso (se han especificado todos los datos necesarios). Seleccione el tipo de gráfico para el informe en la lista Tipo de gráfico.
4. Pulse Siguiente para abrir el panel Parámetros de presentación de informe.
   - Revise los parámetros, que varían para cada tipo de diagrama.
   - Opcionalmente, altere temporalmente cualquiera de los valores predeterminados para el tipo de gráfico seleccionado.
5. Pulse Siguiente para continuar al panel Enviar informe, y continúe con el procedimiento Enviar definición de informe.
6. Para ver el informe gráfico, vaya a Mis paneles de control y añada el informe gráfico.

Nota:

Aparecerá un icono de renovación en todos los informes gráficos junto al icono de ayuda.

Enviar definición de informe

1. Opcionalmente, añada comentarios (consulte Comentarios).
2. Opcionalmente, asigne roles (consulte Roles de seguridad).
3. Pulse Guardar.

Modificar un informe

1. Busque el informe que se va a modificar. Vaya al menú buscador de Creador de informes.
2. Pulse Modificar para abrir el panel Columnas de informe.
3. Continúe con Personalizar la Presentación de informe.

Clonar un informe

1. Busque el informe que desea clonar. Vaya al menú buscador de Creador de informes.
2. Pulse Clonar para abrir el panel Columnas de informe.
3. Especifique un nombre nuevo para el informe clonado, en el recuadro Título del informe. Puede especificar el nuevo nombre en cualquiera de las pantallas subsiguientes, el único requisito es que el nombre nuevo se debe especificar antes de que se pueda guardar el informe clonado.
4. Continúe con Personalizar la Presentación de informe.

Eliminar un informe

Tenga en cuenta que no puede eliminar informes predefinidos y no puede eliminar los informes que se utilizan en los procesos de auditoría.

1. Busque el informe que se va a eliminar.
2. Pulse Suprimir para eliminar el informe.

Limitación del tamaño del informe

Los informes tabulares están limitados a 5.000 filas de salida, pero cuando se incluyen en un proceso de flujo de trabajo, se puede exportar cualquier número de filas desde la tarea de informe a un archivo CEF o CSV. Consulte Creación de procesos de auditoría.

Límites

El límite para los botones cuando se visualiza un informe (generar PDF, generar CSV e imprimible) es de 30.000 filas. No es personalizable.

El límite para la consulta Cumplimentar desde consulta en el Creador de grupos y el Creador de alias cuando se ejecuta a través de Ejecutar una vez ahora es de 5.000 filas. No es personalizable.

El límite para Cumplimentar desde consulta en el Creador de grupos y el Creador de alias cuando se ejecuta a través de Planificación es de 20.000 filas. Este límite es personalizable, mediante el mandato de CLI, show/store populate_from_query_maxrecs.

Modificar el menú Informes profundizables para un informe

De forma predeterminada, el menú desplegable para un informe incluye todos los informes con parámetros de tiempo de ejecución que pueden proporcionar los atributos del informe, al que se da las restricciones de rol de seguridad normales. Para inhabilitar o habilitar cualquier informe en el menú desplegable para un informe:

1. Localice el informe. Vaya al menú buscador de Creador de informes.
2. Pulse Control profundizable para abrir el panel Control profundizable del informe.
3. Marque el recuadro de selección para que se inhabilite cualquier informe, o desmarque el recuadro de selección para que se habilite cualquier informe.
4. Pulse Aplicar. El sistema muestra un mensaje que indica que los cambios se han aplicado satisfactoriamente.
5. Pulse Hecho cuando haya terminado.

Asignación de API

De forma predeterminada, la aplicación Guardium se proporciona con datos de configuración que enlaza muchas de las funciones de la API con informes; proporcionando a los usuarios, a través de la interfaz gráfica de usuario, llamadas preparadas a las API a partir de datos de informes. Utilice la Asignación de API para enlazar funciones adicionales de la API con informes de Guardium o informes personalizados.

Para obtener más información sobre cómo utilizar las funciones de la API enlazada, consulte la documentación sobre la generación de entradas de GuardAPI.

1. Localice el informe. Vaya al menú buscador de Creador de informes.
2. Pulse Asignación de API para abrir el panel Asignación de API, que muestra las funciones actuales de la API que están correlacionadas con el informe seleccionado.
3. Pulse una función de API para visualizar una ventana emergente de la API actual a Correlaciones de parámetros de informe; mostrando los parámetros de la API, si son necesarios los parámetros de la API, los valores predeterminados y si alguno de los campos de informe está correlacionado actualmente con esos parámetros.

   Si no hay campos en el informe que estén enlazados a parámetros de API, puede que sea irrelevante enlazar una función de API con un informe. La correlación de los parámetros de la API con los campos del informe se puede llevar a cabo a través de la interfaz gráfica de usuario y Guardium CLI. Para obtener información adicional sobre los parámetros de la API de correlación con campos de informe, consulte Correlación de parámetros de GuardAPI con atributos y entidades de dominio en la sección Generación de entradas de GuardAPI.

4. Pulse en el signo de mayor que '>' para añadir la función seleccionada de la API a la lista actual de funciones que están asignadas a este informe.
5. Pulse Aplicar para guardar los cambios.

Abrir consulta para editar desde el portlet de informe

1. Abra un portlet de informe para cualquier informe que esté basado en la consulta que se va a editar.
2. Pulse Editar esta consulta de informe en la barra de herramientas. Debe estar autorizado para modificar la consulta en la que se basa el informe.

- Parámetros de informe
  Puede utilizar parámetros para controlar el contenido y la presentación de un informe.
- Creación de paneles de instrumentos
  Puede crear uno o varios paneles de control, añadir informes a los mismos y configurar su aspecto.
- Visualización de un informe
  Hay varias formas de visualizar un informe, incluido el panel de control y la búsqueda de interfaz de usuario.
- Creación de un informe
  Si los informes predefinidos no satisfacen sus necesidades, puede crear los suyos propios.
- Creación de informes para z/OS
  Aprenda a crear informes Guardium para fuentes de datos z/OS mediante la personalización de informes incorporados y consultas de ejemplo.
- Despensa de datos
  Una despensa de datos es un tipo de almacén de datos. Un almacén de datos agrega y organiza los datos de una forma genérica que se pueden utilizar posteriormente para informes y análisis. Una despensa de datos comienza con un análisis de datos definido por el usuario y hace énfasis en satisfacer las demandas específicas del usuario en términos de contenido, presentación y facilidad de uso.
- Auditoría e informes
  Guardium organiza los datos que recopila en un conjunto de dominios. Cada dominio contiene un tipo diferente de información relativa a un área específica de interés: acceso a datos, excepciones, infracciones de política, etc.
- Consultas
  Utilice una de las muchas consultas predefinidas que vienen con Guardium para obtener información sobre los datos. Utilice el Creador de consultas para trabajar con consultas.
- Dominios, entidades y atributos
  Un dominio proporciona una vista de los datos que Guardium almacena.

- Cómo sacar provecho de los informes predefinidos
  En lugar de crear informes personalizados desde cero, aproveche el contenido predefinido en la aplicación Guardium.
- Cómo formular preguntas de los datos
  Utilice el Creador de consultas para definir y modificar preguntas sobre los datos recopilados.
- Cómo informar sobre columnas y tablas latentes
  Guardium ofrece una funcionalidad que puede ayudar a los arquitectos de datos y DBA a descubrir qué tablas y qué campos no se están utilizando.
- Cómo generar la Llamada de API desde Informes
  Generar llamadas de API de Guard desde un informe, ya sea desde una sola fila dentro de un informe o basándose en el informe
- Cómo utilizar Constantes en Llamadas de API
  Cree un atributo de entidad nuevo que se utilizará durante una llamada de función de API.
- Cómo utilizar llamadas de API desde informes personalizados
  Enlace funciones de API con informes y correlacione campos de informe con los parámetros funcionales de la API.
- Canal de información externo opcional
  Los canales de información externos le permiten enviar los datos del informe de Guardium directamente a una base de datos externa.
- Correlación de un canal de información externo
  Aprenda a correlacionar un canal de información externo para enviar datos de informes de Guardium directamente a una base de datos externa.
- Creador de informes distribuidos
  Esta característica Gestor central proporciona una forma de recopilar automáticamente datos de todas las unidades gestionadas de Guardium o de un subconjunto de las mismas que están asociadas con este Gestor central. Los informes distribuidos están diseñados para proporcionar una vista de alto nivel, para correlacionar datos de orígenes de datos y, para resumir vistas de los datos. Continuaría utilizando agregadores para la recopilación de datos a nivel de fila entre los recopiladores.
- Cómo crear un Informe distribuido
  Guardium ofrece una función que proporciona una forma de recopilar datos automáticamente de todas las unidades gestionadas de Guardium o de un subconjunto de unidades que están asociadas con un Gestor central de Guardium.

Parámetros de informe

Puede utilizar parámetros para controlar el contenido y la presentación de un informe.

Hay dos tipos de parámetros de informe:

- Un *parámetro de tiempo de ejecución* proporciona un valor que debe utilizarse en una condición de consulta. Existe un conjunto predeterminado de parámetros de tiempo de ejecución para todas las consultas, y se puede definir cualquier número de parámetros de tiempo de ejecución en la consulta utilizada por el informe.
- Un *parámetro de presentación* describe una característica física del informe; por ejemplo, si un informe gráfico incluye una leyenda o etiquetas, o los colores que se deben utilizar para un elemento. Todos los parámetros de presentación se proporcionan con los valores iniciales cuando se define un informe.

Para establecer parámetros de informe:

1. Pulse Configurar parámetros de informe a partir de las opciones incluidas en el informe. Consulte el icono .
2. En el panel, especifique los parámetros de ejecución y de presentación en los recuadros que se proporcionan, según sea necesario, para que se lleve a cabo la tarea.
3. Pulse Guardar.
4. Para ver el informe, vaya a Mis paneles de control.

Parámetros de tiempo de ejecución estándares

Los siguientes parámetros de tiempo de ejecución están presentes para todos los informes.

Parámetro de tiempo de ejecución	Valor predeterminado y descripción
QUERY_FROM_DATE	Ninguno para un informe nuevo, varía para los informes predeterminados. La fecha de inicio para el informe siempre es necesaria.
QUERY_TO_DATE	Ninguno para un informe nuevo, varía para los informes predeterminados, aunque el valor predeterminado es casi siempre NOW. Esta fecha es la fecha final para el informe, y siempre es necesaria.
REMOTE_SOURCE	Ninguno. En un entorno de Gestor central, puede ejecutar un informe en una unidad gestionada seleccionando dicho sistema Guardium en la lista Fuente de datos remota.
SHOW_ALIASES	Ninguno (es decir, se utiliza el valor predeterminado de todo el sistema). Seleccione el Activado para mostrar siempre los alias, o Desactivado para no mostrar nunca alias. Seleccione el botón predeterminado para revertir al valor predeterminado de todo el sistema (controlado por el administrador) después de haber utilizado el botón Activado o Desactivado.

Mandato de informe de GuardAPI para devolver una lista de nombres de parámetros de tiempo de ejecución

Utilice este mandato de GuardAPI, list_parameter_names_by_report_name. Esta función toma un nombre de informe como parámetro de entrada y devuelve una lista de nombres de parámetros de ejecución para dicho informe.

Tema principal: Informes

Creación de paneles de instrumentos

Puede crear uno o varios paneles de control, añadir informes a los mismos y configurar su aspecto.

Antes de empezar

Piense en cómo desea organizar los informes que ve con regularidad. ¿Desea verlos en un panel de control o en varios paneles de control? ¿Desea agruparlos y ordenarlos de acuerdo con su propósito, lo críticos que son o algún otro enfoque? Siempre puede reorganizar los paneles de control o crear unos nuevos.

Acerca de esta tarea

Procedimiento

1. Pulse Mis paneles de control > Crear panel de control nuevo para abrir un nuevo panel de control.
2. Especifique un nombre descriptivo en el campo Nombre. Este nombre se utiliza en la lista de paneles de control del menú.
3. Pulse Añadir informe para visualizar una lista de los informes disponibles. Si ha designado determinados informes como favoritos, puede seleccionar el recuadro Mis favoritos para ver sólo una lista de esos informes. Si desea ver sólo informes gráficos, seleccione el recuadro Sólo gráfico.
4. El diálogo Añadir un informe muestra una lista de todos los informes que cumplen sus criterios. Puede examinar la lista de informes, o escribir una serie en el campo Filtrar. La lista de informes se actualiza a medida que escribe.
5. Pulse el título de un informe para añadirlo al panel de control. Continúe añadiendo tantos informes como desee. Cuando haya acabado de añadir informes, pulse Cerrar.

Resultados

Dispone de un panel de control que le proporciona un acceso sencillo a algunos informes seleccionados.

Qué hacer a continuación

Revise el aspecto del panel de control. ¿Es fácil de utilizar, y para encontrar la información que desea? Si no es así, puede configurarlo más.
Tema principal: Informes

Configuración del panel de control

Puede configurar varios aspectos de la apariencia del panel de control para que sea lo más útil posible.

Acerca de esta tarea

Piense en cómo utiliza los informes. ¿Qué acuerdo hace que sea más fácil alcanzar sus objetivos? Experimente con estos cambios.

Procedimiento

1. Reorganice los informes. Para mover un informe, coloque el cursor en la barra de título del informe y arrástrelo a una nueva ubicación.
2. Elija un nuevo número de columnas pulsando 1, 2, o 3 en el área Número de columnas. De forma predeterminada, los informes se muestran en dos columnas. Si necesita más espacio para cada informe, pulse 1 para ver cómo se ven los informes cuando tienen el ancho completo del panel de instrumentos. Si prefiere ver más informes a la vez, pruebe con tres columnas.
3. Cambie el tamaño de los informes. Arrastre el icono de cambio de tamaño para hacer que un informe sea más largo o más corto, más estrecho o más ancho. Si ajusta la anchura de un informe, todos los informes de dicha columna utilizarán la nueva anchura. Si cambia el número de columnas, todas las columnas volverán a sus anchuras predeterminadas.

Utilización del panel de control

Utilice los pasos para añadir un informe al panel de control y, a continuación, para personalizar el aspecto.

Acerca de esta tarea

El panel de control sustituye a Añadir a panel y Añadir a Mis informes.

Procedimiento

1. Pulse en el icono Panel de control en la navegación.
2. A continuación, pulse Crear panel de control nuevo.
3. Pulse Añadir informe para seleccionar un informe de todos los informes a los que tiene acceso, incluidos todos los informes nuevos que haya creado.
4. Aproveche el filtrado para encontrar rápidamente el informe en el que está interesado.
5. Pulse el nombre del informe para añadirlo al panel de control. Añada tantos informes a su panel de control como desee, sólo seleccionando cada informe.
6. Personalice el panel de control seleccionando un diseño. El valor predeterminado es de dos columnas. Una columna: los informes asumirán el ancho del panel de control. Dos columnas: los informes asumirán la mitad de la anchura del panel de control. Tres columnas: los informes asumirán un tercio de la anchura del panel de control.
7. Personalice el panel de control moviendo los informes dentro de la pantalla. Utilice el icono para personalizar el gráfico.
8. Designe informes específicos como favoritos seleccionando el icono . Al añadir informes a un panel de control, filtre en función de los favoritos o en función de los gráficos.
9. Asigne un nombre al panel de control pulsando en el icono de edición.
10. Suprima un panel de control, pulsando el icono de supresión .

Visualización de un informe

Hay varias formas de visualizar un informe, incluido el panel de control y la búsqueda de interfaz de usuario.

Puede ver un informe de varias formas:

- Si ha guardado el informe en un panel de control, abra el panel de control para ver el informe.
- Puede añadir el informe a un panel de control. Abra el panel de control y pulse Añadir informe y, a continuación, elija el informe en la lista.
- Algunos informes se listan en categorías en el ciclo de vida de informes.
- Algunos informes se listan bajo el ciclo de vida para el que son más relevantes.
- Puede utilizar la función de búsqueda de la interfaz de usuario (UI) para buscar el informe. En el banner, elija Interfaz de usuario en la lista desplegable situada junto al recuadro Buscar. Especifique el nombre del informe en el recuadro de búsqueda. Los resultados empiezan a aparecer después de escribir unos pocos caracteres. Elija el informe de la lista de resultados.

Las opciones siguientes (con iconos) permiten la edición y la configuración del informe:

- Edite la consulta para este informe
- Proceso ad-hoc para Ejecutar una vez ahora: Utilice esto para invocar una llamada a mandatos GuardAPI.
- Abrir en una ventana nueva
- Configurar columnas de informe
- Configurar parámetros de tiempo de ejecución: Un parámetro de tiempo de ejecución proporciona un valor que se utilizará en una condición de consulta. Existe un conjunto predeterminado de parámetros de tiempo de ejecución para todas las consultas, y cualquier número de parámetros de tiempo de ejecución se puede definir en la consulta utilizada por el informe.
- Añadir a favoritos
- Renovar

Puede ocultar columnas de la vista. Pulse en el icono de columnas y quite la marca de los recuadros de selección para las columnas que desea ocultar.

Puede ordenar los datos del informe por el contenido de cualquier columna. Pulse el título de la columna en la que desea ordenar. Para invertir el orden, pulse de nuevo en el título. Siempre se realiza la ordenación en los valores de datos reales, ignorando los alias que se hayan definido.

Puede imprimir un informe mientras lo está visualizando. Pulse Exportar > Informe imprimible completo para abrir una copia imprimible del informe en un separador nuevo. Pulse el icono de impresora en el separador nuevo para imprimir el informe. También puede imprimir un informe exportándolo a un archivo PDF e imprimiendo el archivo PDF.
Nota: Para una instancia en la que el texto PDF es demasiado pequeño para leer, el informe PDF tiene un límite físico en cuanto al tamaño que puede expandirse horizontalmente la página. Dado que cada línea del informe PDF debe caber en una línea, el tamaño de la letra cambia para ajustarse a los datos, y puede forzar un tamaño de tipo de letra muy pequeño para visualizar todos los datos.

Los informes gráficos se pueden personalizar pulsando el icono Personalizar gráfico. Las opciones incluyen convertir los datos en un gráfico de líneas, cambiar la orientación del eje X e Y, convertir el informe en un gráfico circular o en un gráfico de columnas apiladas.

Al visualizar informes que muestran información de Oracle, ocasionalmente el carácter de signo de interrogación se utiliza para informar al visor de que la información de inicio de sesión no estaba disponible. De nuevo al visualizar informes que muestran información de Oracle, el aspecto del número -1 significa que se ha visto afectado un número de registros desconocido. Se registran todas las sesiones de Oracle, incluso con los inicios de sesión que faltan.

Problema: el campo de usuario de SO está vacío en los informes de IBM Security Guardium

Nota para las plataformas UNIX/Linux

Conexiones remotas: el usuario del SO no es un campo obligatorio para conectarse a la base de datos. Por lo tanto, depende del cliente de la base de datos enviarlo con el paquete de inicio de sesión. Si no se envía la información de USER de SO, este campo estará vacío. Si la serie de conexión de cliente incluye información sobre el propietario del proceso, se utilizará para llenar el campo USER de SO.

Conexiones locales: la misma limitación se aplica a las conexiones ejecutadas localmente. Sin embargo, cuando las conexiones con la base de datos se realizan localmente, Guardium proporciona una forma de identificar la información de USER de SO mediante la habilitación de la cadena de UID. Tenga en cuenta que la cadena de UID puede estar asociada con alguna sobrecarga de S-TAP adicional y se debe tener en cuenta caso por caso, cuando sea necesario.

La cadena de UID está soportada con protocolos EXIT (nota, para la salida de DB2, necesita un nivel de parche específico).

La cadena de UID está soportada con ATAP para MongoDB, Teradata y Sybase ASE (con IP reales).

plataforma Windows

Conexiones remotas: el usuario del SO no es un campo obligatorio para conectarse a la base de datos. Por lo tanto, depende del cliente de la base de datos enviarlo con el paquete de inicio de sesión. Si no se envía la información de USER de SO, este campo estará vacío.

Conexiones locales: la plataforma Windows siempre recogerá al usuario del SO que ejecuta el proceso que se ha conectado con el propietario del proceso de BD (no es necesaria ninguna cadena de UID en Windows).

- Renovación de informes
  Algunos informes están configurados para renovar automáticamente sus datos. En otros informes, puede renovar los datos manualmente a través de la interfaz de usuario.
- Exportación de un informe
  Puede exportar un informe a un archivo PDF o a un archivo de valores separados por comas.
- Visualización de informes profundizables
  Muchos informes proporcionan acceso a informes profundizables que proporcionan datos más granulares.

Tema principal: Informes

Renovación de informes

Algunos informes están configurados para renovar automáticamente sus datos. En otros informes, puede renovar los datos manualmente a través de la interfaz de usuario.

Cuando se visualiza un informe que está configurado para renovarse automáticamente, el color del icono Renovación de flechas circulares para este informe es verde, lo que indica que el informe se está renovando automáticamente.

En un determinado punto, el informe deja de renovarse si no se realizan cambios adicionales en el informe y el color del icono de renovación pasa de verde a rojo. El punto en el tiempo en el que el color cambia es igual a la mitad del tiempo de espera excedido de la sesión de la interfaz gráfica de usuario (que se puede encontrar ejecutando el mandato de CLI, mostrar tiempo de espera de sesión).

Por ejemplo, si el tiempo de espera de sesión es el valor predeterminado 900 segundos, el icono Renovación de flechas circulares en el informe Tasa de solicitudes es verde durante 450 segundos y, a continuación, se vuelve rojo.

Hay varias formas de renovar los datos de informes manualmente:

- Pulse Renovar en la barra de herramientas.
- Utilice cualquier botón de la barra de herramientas para imprimir un informe, descargar datos de informe, o grabar el informe en un archivo PDF. Los datos del informe se renuevan antes de realizar cualquiera de estas acciones.
- Establezca un intervalo de tiempo para la renovación periódica, estableciendo el valor del parámetro refreshRate. Para realizar esta tarea:
  - Pulse Personalizar en la barra de herramientas del informe.
  - En el diálogo Configuración, establezca el parámetro refreshRate en el número de segundos después de los cuales se van a actualizar los datos del informe. El valor predeterminado de cero indica que los datos del informe no se renuevan de forma planificada.
  - Pulse Aceptar.

Personalizar informes

Cuando el usuario edita un informe o realiza una modificación en el informe mediante Personalización de informes, el usuario debe pulsar manualmente Renovar. No hay ninguna renovación automática.

Personalización de la interfaz de usuario: En el diálogo "Nuevo ciclo de vida" y "Nuevo grupo", los grupos están limitados a un máximo de 5 niveles de profundidad, por lo que incluso con nombres de grupo más largos, todos los niveles de nombres de grupo y texto de elemento de nodo son visibles en el panel de navegación.

Personalización de la interfaz de usuario: Cuando el usuario especifica "<" o ">" en el recuadro de texto del diálogo "Nuevo ciclo de vida" o "Grupo nuevo", se visualiza un mensaje emergente para indicar que "El nombre no puede contener los caracteres especiales < ni >" y el botón "Aceptar" queda inhabilitado.

Personalización de la interfaz de usuario: En el diálogo "Nuevo ciclo de vida" y el diálogo "Grupo nuevo", el usuario puede escribir un máximo de 50 caracteres en el recuadro de texto.

Tema principal: Visualización de un informe

Exportación de un informe

Puede exportar un informe a un archivo PDF o a un archivo de valores separados por comas.

Puede exportar el contenido de un informe a un archivo PDF (Portable Document Format) y guardar el archivo o visualizarlo. En la barra de herramientas de informe, pulse Exportar > Descargar como PDF para crear una copia en PDF. Siga la solicitud para guardar o ver el archivo.

Cuando se genera un archivo PDF grande, el proceso puede hacer que la interfaz de usuario exceda el tiempo de espera. Si tiene previsto generar archivos PDF de gran tamaño, considere hacerlo como parte de un proceso de auditoría o aumentando el valor de tiempo de espera de la interfaz de usuario para evitar este problema.

También puede exportar el contenido de un informe a un archivo de valores separados por comas (csv). Puede exportar todos los registros (todo el informe) en el informe, o sólo los registros de visualización (los datos visualizados actualmente).

En la barra de herramientas de informe, pulse Exportar > Bajar todos los registros o Exportar > Bajar registros de visualización. Puede guardar los resultados o seleccionar una aplicación en la que verlos.

Nota: Si edita un informe y elimina una columna (por ejemplo, editando un informe con siete columnas y eliminando una columna, dejando seis columnas), cuando el informe se exporte como un archivo PDF, el informe mostrará las siete columnas originales.

Tema principal: Visualización de un informe

Visualización de informes profundizables

Muchos informes proporcionan acceso a informes profundizables que proporcionan datos más granulares.

Si alguna acción de detallar más está disponible en un informe tabular, el usuario lo sabrá pulsando con el botón derecho del ratón en una fila de la cuadrícula y aparecerá un menú contextual con las acciones de detallar más disponibles.

Para que esté disponible como un informe detallado:

- Todos los parámetros de tiempo de ejecución para el informe detallado deben estar disponibles desde el informe que se está visualizando.
- Si se han asignado roles de seguridad, debe tener acceso al informe detallado.

Modificar el menú Informes profundizables para un informe

De forma predeterminada, el menú desplegable para un informe incluye todos los informes con parámetros de tiempo de ejecución que pueden proporcionar los atributos del informe, al que se da las restricciones de rol de seguridad normales. Para inhabilitar o habilitar cualquier informe en el menú desplegable para un informe:

1. Localice el informe. Vaya al menú buscador de Creador de informes.
2. Pulse Control profundizable para abrir el panel Control profundizable del informe.
3. Marque el recuadro de selección para que se inhabilite cualquier informe, o desmarque el recuadro de selección para que se habilite cualquier informe.
4. Pulse Aplicar. El sistema muestra un mensaje que indica que los cambios se han aplicado satisfactoriamente.
5. Pulse Hecho cuando haya terminado.

Tema principal: Visualización de un informe

Creación de un informe

Si los informes predefinidos no satisfacen sus necesidades, puede crear los suyos propios.

Antes de empezar

Puede elegir una consulta en la que se basa este informe y el dominio de la consulta. Si tiene que crear una consulta nueva, hágalo antes de crear un informe basado en ella. Recuerde que hay una distinción entre consultas e informes. Una consulta describe un conjunto de información que se debe obtener de los datos recopilados. Un informe describe cómo se presentan los datos devueltos por la consulta. Consulte Utilización del Creador de consultas para obtener más información sobre la creación de una consulta. Consulte Dominios, entidades y atributos para obtener más información sobre cómo trabajar con dominios.

Acerca de esta tarea

Puede que encuentre más sencillo clonar un informe y modificarlo que crear un informe desde cero.

Procedimiento

1. Pulse Informes > Herramientas de configuración de informes > Creador de informes para abrir el buscador del Creador de informes o el menú Filtrar. Si selecciona Buscar en este punto sin elegir ningún dominio ni consulta, aparecerá un menú con todas las consultas listadas. Seleccione una consulta y utilice los iconos (Añadir nuevo informe , Modificar , Clonar , o Suprimir) para trabajar con las consultas.
2. En el menú buscador Creador de informes, pulse Nuevo .
3. Aparece el menú Crear informe. Seleccione una consulta y proporcione un nombre al informe. A continuación, pulse Siguiente.
4. La siguiente pantalla devuelve las columnas de tabla de la consulta seleccionada. Personalícelas o utilícelas tal cual. A continuación, pulse Siguiente.
5. Aparece el menú Atributos de informe. Elija un tipo de informe, ya sea tabular o gráfico. A continuación, pulse Siguiente.
6. A continuación, envíe el informe para su creación pulsando Guardar. Aparecerá una pantalla de acuse de recibo que indica que los datos se han guardado satisfactoriamente.

Qué hacer a continuación

Si desea incluir este informe en un panel de control, abra el panel de control, pulse Añadir informes, y seleccione este informe en la lista.
Tema principal: Informes

Creación de informes para z/OS

Aprenda a crear informes Guardium para fuentes de datos z/OS mediante la personalización de informes incorporados y consultas de ejemplo.

Mientras que el proceso de creación de informes para orígenes de datos de z/OS es el mismo que para otras bases de datos, no siempre hay una correlación directa entre los conceptos de sistema principal y los atributos y las entidades de creación de informes de Guardium. Para facilitar la comunicación entre los auditores y el personal del sistema principal, en esta sección se describe la correlación de datos de sucesos de sistema principal con atributos y entidades de Guardium. Hay algunos informes incorporados que se pueden personalizar, y esta información describe las consultas adicionales que son útiles para los escenarios típicos de la auditoría.

Tema principal: Informes
Conceptos relacionados:
Dominios, entidades y atributos
Utilización del Creador de consultas
Entidades y atributos

Despensa de datos

Una despensa de datos es un tipo de almacén de datos. Un almacén de datos agrega y organiza los datos de una forma genérica que se pueden utilizar posteriormente para informes y análisis. Una despensa de datos comienza con un análisis de datos definido por el usuario y hace énfasis en satisfacer las demandas específicas del usuario en términos de contenido, presentación y facilidad de uso.

Utilice esta función para:

- Definir y generar una despensa de datos.
- Agregar datos resumidos y analizados de todas las unidades para habilitar la vista de nivel alto/corporativa en un tiempo de respuesta razonable.
- Mejorar el rendimiento de los informes en línea en Agregadores de Guardium.
- Proporcionar capacidades de análisis interactivo para buscar patrones, tendencias y valores atípicos.
- Habilitar la contracción y expansión de niveles de datos

Una despensa de datos es práctica y eficiente para todos los informes predefinidos de Guardium. Prepara los datos con antelación para evitar la sobrecarga, las exploraciones completas y el bajo rendimiento.

El icono Configuración de despensa de datos está disponible en cualquier informe predefinido.

Puntos destacados de las ventajas:

- Proporcionar la prestación analítica de Guardium que da soporte al ciclo de vida completo del análisis de datos.
- El proceso analítico se inicia desde el Creador de consultas y el Creador de tablas de pivote donde los usuarios definen sus necesidades de análisis de datos y, a continuación, "Establecer como despensa de datos".
- El programa de extracción de la despensa de datos se ejecuta por lotes de acuerdo con la planificación especificada. Resume los datos por horas, días, semanas o meses según la granularidad solicitada y, a continuación, guarda los resultados en una tabla nueva en la base de datos de analíticas de Guardium.
- A continuación, los datos son accesibles para los usuarios a través de los programas de utilidad de Informes estándar y Proceso de auditoría e, igualmente, para cualquier otra Entidad/ Dominio tradicional. Los datos de extracción de la despensa de datos están disponibles bajo el dominio DM. El nombre de entidad se establece de acuerdo con el nuevo nombre de tabla especificado para los datos de la despensa de datos. Utilizando el Creador de consultas y el Creador de informes, los usuarios pueden clonar la consulta predeterminada y editar la consulta e informe, generar portlets y añadirlos a un panel.
- El resumen de los datos reduce significativamente el volumen de datos. Elimina las uniones de muchas tablas mediante el almacenamiento del análisis de datos en una tabla no normalizada y precalculada.

- La vista corporativa se soporta utilizando el programa de utilidad Agregación estándar para las nuevas tablas de analítica de Guardium. Si existe una gran cantidad de datos de fila detallados en los niveles superiores de la Jerarquía de agregación, la característica Agregación selectiva, que permite la agregación de módulos específicos, se puede configurar sólo para agregar datos de analítica.

Se puede acceder al Constructor de despensa de datos a través del Creador de consultas, los Resultados de los informes y la vista de Tabla de pivote.

Seleccione el icono Establecer como despensa de datos. El botón está disponible sólo después de Guardar.

El acceso a la pantalla está habilitado para usuarios con permiso de Creación de despensa de datos (Permiso de rol de usuario). Muestre el botón nuevo Establecer como despensa de datos sólo para los usuarios con el permiso adecuado.

Persistencia de la Despensa de datos: Los cambios en la Consulta, Informe o Tabla de pivote originales no afectan a la Despensa de datos. Se guarda una instantánea de la definición de análisis originada junto con la Despensa de datos al crearse.

Si la Despensa de datos se basa en la Tabla de pivote, el proceso de extracción no calcula la línea Total (la suma de las columnas) y el Porcentaje de columna no está soportado.

Además de la definición de la Despensa de datos, el proceso Definición de despensa de datos crea lo siguiente:

- Entidad y dominio nuevos
- Consulta predeterminada
- Informe y portlet predeterminados
- Nueva tabla de Despensa de datos en la nueva base de datos “DATAMART” para almacenar los datos extraídos

Despensa de datos: Creador de consultas e informes

El proceso de definición de Despensa de datos crea un nuevo Dominio, Entidad, Consulta e Informe predeterminados. Se puede acceder a la Consulta e Informe predeterminados a través del menú Creación de informes.

Al pulsar Despensa de datos se abre la interfaz gráfica de usuario del Buscador de consultas; los campos Consulta, Informe y Entidad filtrarán sólo los dominios de la Despensa de datos (el nombre de dominio empieza por: DatamartDefinition.DOMAIN_PREFIX).

Interfaz gráfica de usuario del Creador de informes: Los informes de Despensas de datos predeterminados y todos los demás informes que están relacionados con los dominios de Despensas de datos están disponibles en la interfaz gráfica de usuario del Creador de informes.

Siga estos pasos:

1. Como usuario Administrador, seleccione el icono Despensa de datos .
2. Seleccione Nuevo para crear una nueva Despensa de datos o seleccione en la lista de Despensas de datos creadas anteriormente.
3. Complete los campos que solicitan el nombre de la Despensa de datos y el nombre de la Tabla (el valor predeterminado es DM). Especifique una granularidad de tiempo y seleccione una hora de inicio inicial en el icono de calendario. La descripción es opcional.
4. Utilice el Planificador para planificar cuándo ejecutar esta función (Ejecutar una vez ahora).
5. Utilice la sección Roles para restringir Despensa de datos sólo a los usuarios con el permiso adecuado.
6. Guarde la configuración.

   Nota: Los cambios en la consulta/informe originados no afectan a la Despensa de datos existente.
   Nota: Cuando se ejecuta una extracción de despensa de datos (Planificada o Ejecutar una vez ahora) por primera vez, extrae datos de la Fecha de inicio a la hora actual en función de la Granularidad de tiempo. Guarda el siguiente period from en la tabla DM_EXTRACTION_STATE. En la siguiente ejecución, se extraen los datos a partir del siguiente period from. Si se busca una extracción de despensa de datos antes del siguiente period from, entonces la extracción de la despensa de datos se mostrará como vacía, porque la extracción ya ha procesado ese periodo de tiempo. Para poder extraer datos antes del siguiente period from, restaure los datos antiguos y, a continuación, ejecute de nuevo la despensa de datos.

Gestión central y Despensa de datos

En un entorno de Gestión central, la configuración se distribuye automáticamente a las unidades gestionadas.

La planificación de extracción se puede modificar en una Unidad gestionada.

En el caso de varios Gestores centrales, la definición de la Despensa de datos se puede clonar utilizando la prestación de Exportación/Importación.

Añadir planificación de Extracción de despensa de datos a la pantalla Distribución de gestor central.

Extracción de Despensa de datos

Datos extraídos:

1. Export of: Exception Log - detalla las Excepciones/Errores capturados por Guardium. El registro incluirá la descripción de excepción/error, el nombre de usuario, la dirección de origen, el protocolo de BD, etc.
2. Export of: Session Log - Incluye detalles sobre las sesiones de los orígenes de datos (iniciar sesión para cerrar sesión). El registro incluye las indicaciones de fecha y hora de inicio y de fin de sesión, el usuario de BD y de SO de la sesión, el programa de origen, etc.
3. Export of: Session Log Ended - La sesión puede extenderse durante un periodo largo. La extracción funciona cada hora. Este registro envía las sesiones que finalizaron más tarde de la hora de inicio.
4. Export of: Access Log - Incluye detalles de la información de conexión y el resumen de actividad por hora. El registro incluye el usuario de BD y de SO, los SQL satisfactorios y anómalos, el IP de servidor y cliente, etc.
5. Export of: Full SQL - este registro incluye los detalles de SQL ejecutados. El registro incluye SQL completo, los registros afectados, el ID de sesión, etc.
6. Export of: Outliers List - este registro incluye los valores atípicos. El registro incluye la IP de servidor, el usuario de BD, el tipo de valor atípico, BD, etc.
7. Export of: Outliers Summary - este registro incluye un resumen de horas de valores atípicos. El registro incluye el IP de servidor, el usuario de BD, BD, etc.

8. Export of: Group Members - Incluye un registro de todos los miembros de grupo. El registro incluye el Tipo de grupo, la Descripción de grupo, el Miembro de grupo y el Distintivo de tupla.
9. Export of: Export Extraction Log - Incluye el registro de datos relevantes para todos los archivos de copia o exportación con un nombre que empiece por "Export:".
10. Export of: Policy Violations - Se registra una infracción de política cada vez que se desencadena una regla de política. Este registro incluye los detalles acerca de las infracciones registradas como, por ejemplo, Usuario de BD, Programa de origen, Descripción de regla de acceso, Serie SQL completa, etc.
11. Export of: Buff Usage Monitor - Proporciona un conjunto amplio de estadísticas de uso de almacenamiento intermedio de sniffer
12. Export of: VA Results - Proporciona Resultados de VA
13. Export of: Policy Violations - Detallado – igual que el Exportar registro de extracción, pero tiene tuplas de Objeto/Verbo. Se recomienda utilizar sólo uno de ellos.
14. Export of: Access Log - Detallado - igual que Registro de acceso, pero también tiene los campos siguientes de la entidad Suceso de aplicación: Nombre de usuario de suceso, Tipo de suceso, Serie de valor de suceso, Número de valor de suceso, Fecha de suceso. Se recomienda utilizar dicho Registro de acceso o Registro de acceso - Detallado debería utilizarse y no los dos.
15. Export of: Discovered Instances - Proporciona el resultado de la aplicación S-TAP Discovery, que descubre instancias de base de datos
16. Export of: Databases Discovered –
17. Export of: Classifier Results
18. Export of: Datasources
19. Export of: S-TAP status
20. Export of: Installed Patches
21. Export of: System Info
22. Export of: User – Rol
23. Export:Classification Process Log
24. Export:Outliers List - mejorado
25. Export:Outliers Summary by hour - mejorado

Nombre de despensa de datos	Título del informe	Tipo de unidad	ID de despensa de datos
Export:Access Log	Export: Access Log	Recopilador	22
Export:Session Log	Export: Session Log	Recopilador	23
Export:Session Log Ended	Export: Session Log	Recopilador	24
Export:Exception Log	Export: Exception Log	Cualquiera	25
Export:Full SQL	Export: Full SQL	Recopilador	26
Export:Outliers List	Lista de valores atípicos de analítica	Cualquiera	27
Export:Outliers Summary by hour	Resumen de valores atípicos de analítica		
Por fecha	Cualquiera	28	
Export:Export Extraction Log	Registro de extracción definido por el usuario	Cualquiera	31
Export:Group Members	Export:Group Members	Cualquiera	29
Export:Policy Violations	Export:Policy Violations	Recopilador	32
Export:Buff Usage Monitor	Supervisor del uso de almacenamiento intermedio	Cualquiera	33
Export:VA Results	Exportación del asesoramiento de seguridad	Cualquiera	34
Export:Policy Violations - Detallado	Export:Policy Violations	Recopilador	38
Export:Access Log - Detallado	Export: Access Log	Recopilador	39
Export:Discovered Instances	Instancias descubiertas	Cualquiera	40
Export:Databases Discovered	Bases de datos descubiertas	Cualquiera	41
Export:Classifier Results	Resultados de clasificador	Cualquiera	42
Export:Datasources	Orígenes de datos	Gestor central,	
Autónomo	43		
Export:STAP Status	Supervisor de estado de S-TAP	Recopilador	44
Export:Installed Patches	Parches instalados	Cualquiera	45
Export:System Info	Parches instalados	Cualquiera	46
Export:User - Rol	Usuario - Rol	Gestor central,	
Autónomo	47		
Export:Classification Process Log	Registro de proceso de clasificación	Cualquiera	48
Export:Outliers List - mejorado	Lista de valores atípicos de analítica - mejorada	Cualquiera	49
Export:Outliers Summary by hour - mejorado	Resumen de valores atípicos de analítica por fecha - mejorado	Cualquiera	50

Resumen de problema

El mecanismo de Despensa de datos exporta datos de sniff de Guardium periódicamente en función de la Consulta definida.

Los archivos de salida pueden escribirse en una máquina externa bajo demanda (configurable).

Los Archivos extraídos están comprimidos.

Puede que se haya planificado la extracción (el valor predeterminado es cada hora).

El prefijo de Archivos extraídos es Global_ID y el nombre de host abreviado de origen, Máquina.

Los Archivos extraídos pueden incluir cabeceras de columna (descripciones de atributos).

Cómo se utiliza

Todos los ejemplos que se muestran a continuación son para la Despensa de datos "Export:Exception Log". Para otra extracción, cambie a una de las opciones siguientes:

"Export:Access Log"

"Export:Session Log"

"Export:Session Log Ended"

"Export:Exception Log"

"Export:Full SQL"

"Export:Outliers List"

"Export:Outliers Summary by hour"

"Export:Group Members"

"Export:Export Extraction Log"

"Export:PolicyViolations"

"Export:Buff Usage Monitor"

"Export:VA Results"

"Export:Classifier Results"

"Export:Databases Discovered"

"Export:Access Log - Detallado"

"Export:Discovered Instances"

"Export:Datasources"

"Export:STAP Status"

"Export:Installed Patches"

"Export:System Info"

"Export:User – Rol"

"Export:Classification Process Log"

"Export:Outliers List - mejorado"

"Export:Outliers Summary by hour - mejorado"

Las extracciones de exportación están predefinidas en el sistema (a través del mecanismo de Despensas de datos) y están inhabilitadas de forma predeterminada. Para poder habilitar las extracciones de exportación (todas o específicas), debe planificar las Despensas de datos a través de grdapi, tal como se muestra a continuación. También puede utilizar la interfaz gráfica de usuario para ello.

Trabajo de planificación para la extracción de Despensa de datos:

grdapi schedule_job jobType=dataMartExtraction cronString=”0 1 0/1 ? * 1,2,3,4,5,6,7” objectName=”Export:Exception Log” startTime=”YYYY-MM-DD HH:MM:SS”

Tenga en cuenta que se utiliza startTime para establecer un inicio futuro si es necesario y se puede eliminar si desea iniciar inmediatamente la Despensa de datos.

Para suprimir extracciones de exportación específicas, puede ejecutar lo siguiente

Suprimir trabajo planificado:

grdapi delete_schedule deleteJob="true" jobGroup="DataMartExtractionJobGroup” obname="DataMartExtractionJob_25”

nombretrabajo	**descripción de trabajo/Nombreobjeto**
DataMartExtractionJob_22	Export:Access Log
DataMartExtractionJob_23	Export:Session Log
DataMartExtractionJob_24	Export:Session Log Ended
DataMartExtractionJob_25	Export:Exception Log
DataMartExtractionJob_26	Export:Full SQL
DataMartExtractionJob_27	Export:Outliers List
DataMartExtractionJob_28	Export:Outliers Summary by hour
DataMartExtractionJob_29	Export:Group Members
DataMartExtractionJob_31	Export:Export Extraction Log
DataMartExtractionJob_32	Export:Policy Violations
DataMartExtractionJob_33	Export:Buff Usage Monitor
DataMartExtractionJob_34	Export:VA Results

nombretrabajo	descripción de trabajo/Nombreobjeto
DataMartExtractionJob_38	Export:Policy Violations – Detallado
DataMartExtractionJob_39	Export:Access Log – Detallado
DataMartExtractionJob_40	Export:Discovered Instances
DataMartExtractionJob_41	Export:Databases Discovered
DataMartExtractionJob_42	Export:Classifier Results
DataMartExtractionJob_43	Export:Datasources
DataMartExtractionJob_44	Export:STAP Status
DataMartExtractionJob_45	Export:Installed Patches
DataMartExtractionJob_46	Export:System Info
DataMartExtractionJob_47	Export:User - Rol
DataMartExtractionJob_48	Export:Classification Process Log
DataMartExtractionJob_49	Export:Outliers List - mejorado
DataMartExtractionJob_50	Export:Outliers Summary by hour - mejorado

Puede habilitar o inhabilitar la extracción utilizando el mandato siguiente:

Establecer la Despensa de datos activa:

grdapi datamart_set_active Name=”Export:Exception Log”

Establecer la Despensa de datos inactiva:

grdapi datamart_set_inactive Name=”Export:Exception Log”

Incluir cabecera en la extracción de la Despensa de datos:

Puede determinar si se debe incluir la línea de cabecera (nombres de columna) en el archivo CSV de salida a través de los siguientes grdapi:

grdapi datamart_include_file_header Name=” Export:Exception Log” includeFileHeader=”Yes”

Establecer detalles de host de destino:

Para establecer el host de destino para la extracción de exportación, debe establecer el host de máquina, la vía de acceso y la credencial mediante los siguientes grdapi:

grdapi datamart_update_copy_file_info destinationHost=”Machine_Host” destinationPassword=”********” destinationPath=”/where/to/store/” destinationUser=”user” Name=”Export:Exception Log” transferMethod=”SCP” withCOMPLETEfile=false

El parámetro withCOMPLETEfile es opcional. El valor predeterminado es true. Si se establece en true, el archivo COMPLETE se envía después de que un archivo de datos se haya transferido satisfactoriamente. Consulte la sección “archivo COMPLETE” para obtener más detalles.

Durante la ejecución de este mandato, se enviará un archivo ficticio a una máquina de destino para validar los detalles de conexión. También puede utilizar grdapi de datamart_validate_copy_file_info para ello.

Validar una conexión en un host de destino:

Para validar una conexión con un host de destino, siga grdapi:

grdapi datamart_validate_copy_file_info destinationHost=”Machine_Host” destinationPassword=”********” destinationPath=”/where/to/store/” destinationUser=”user” transferMethod=”SCP”

Puede realizar un seguimiento del registro de extracción a través del informe "Registro de extracción de Despensa de datos" predefinido. El informe está disponible a través de la pantalla Creador de informes; puede añadirla a un panel.

Especifique la opción de personalización en el informe "Registro de extracción de despensa de datos" y defina lo siguiente:

- Especifique un valor para el nombre LIKE: %
- Especifique Period From >=: YYYY-MM-DD HH:MM:SS (especificar una fecha del pasado)
- Especifique el valor para el estado Like: %

Pulse actualizar y el informe de Registro de extracción de DataMart estará activo: le mostrará las últimas extracciones.

Hora de inicio recomendada por el planificador

Las Despensas de datos de valores atípicos deben planificarse unos 10 minutos después de una hora, porque antes de dicho momento los datos no están listos. El proceso de los valores atípicos empieza en una hora.

Tiene sentido planificar el Registro de acceso, el Registro de excepciones, el SQL completo y el Registro de sesiones/Finalizado con algunos intervalos de tiempo. Para obtener los datos coherentes por cada ejecución de Registro de sesión/Finalizado, debe planificarse como los últimos.

Nuestra recomendación

Descripción de trabajo	cronString recomendado	Cada hora a las:
Export:Access Log	0 40 0/1 ? * 1,2,3,4,5,6,7	00:40
Export:Session Log	0 45 0/1 ? * 1,2,3,4,5,6,7	00:45
Export:Session Log Ended	0 46 0/1 ? * 1,2,3,4,5,6,7	00:46

Descripción de trabajo	cronString recomendado	Cada hora a las:
Export:Exception Log	0 25 0/1 ? * 1,2,3,4,5,6,7	00:25
Export:Full SQL	0 30 0/1 ? * 1,2,3,4,5,6,7	00:30
Export:Outliers List	0 10 0/1 ? * 1,2,3,4,5,6,7	00:10
Export:Outliers Summary by hour	0 10 0/1 ? * 1,2,3,4,5,6,7	00:10
Export:Export Extraction Log	0 50 0/1 ? * 1,2,3,4,5,6,7	00:50
Export:Group Members	0 15 0/1 ? * 1,2,3,4,5,6,7	00:15
Export:Policy Violations	0 5 0/1 ? * 1,2,3,4,5,6,7	00:05
Export:Buff Usage Monitor	0 12 0/1 ? * 1,2,3,4,5,6,7	00:12
Export:VA Results	0 0 2 ? * 1,2,3,4,5,6,7	Cada día a las 2 de la madrugada
Export:Policy Violations - Detallado	0 5 0/1 ? * 1,2,3,4,5,6,7	00:05
Export:Access Log - Detallado	0 40 0/1 ? * 1,2,3,4,5,6,7	00:40
Export:Discovered Instances	0 20 0/1? * 1,2,3,4,5,6,7	00:20
Export:Databases Discovered	0 20 0/1? * 1,2,3,4,5,6,7	00:20
Export:Classifier Results	0 20 0/1? * 1,2,3,4,5,6,7	00:20
Export:Datasources	0 0 7 ? * 1,2,3,4,5,6,7	Cada día a las 7 de la madrugada
Export:STAP Status	0 0/5 0/1 ? * 1,2,3,4,5,6,7	Cada 5 minutos
Export:Installed Patches	0 0 5 ? * 1,2,3,4,5,6,7	Cada día a las 5 de la madrugada
Export:System Info	0 0 5 ? * 1,2,3,4,5,6,7	Cada día a las 5 de la madrugada
Export:User - Rol	0 5 0/1 ? * 1,2,3,4,5,6,7	00:05
Export:Classification Process Log	0 25 0/1 ? * 1,2,3,4,5,6,7	00:25
Export:Outliers List - mejorado	0 10 0/1 ? * 1,2,3,4,5,6,7	00:10
Export:Outliers Summary by hour - mejorado	0 10 0/1 ? * 1,2,3,4,5,6,7	00:10

Depurar /var/exportdir

Si una transferencia de archivos falla por algún motivo, por ejemplo, si la máquina de destino está inactiva, entonces vuelve a intentar una transferencia en la siguiente ejecución. El registro de reserva se mantiene en el directorio /var/exportdir. El Proceso de depuración limpia el registro de reserva con una antigüedad superior a 1 día.

Archivo COMPLETE

El archivo COMPLETE vacío se envía para notificar a un sistema externo de que un archivo está preparado.

-Para cada archivo, además del archivo, también se envía un archivo COMPLETE. El nombre del archivo COMPLETE es [nombre de archivo]_COMPLETE.gz

1762144738_gibm32_EXP_SESSION_LOG_20151028230000_COMPLETE.gz

-El proceso es síncrono; por ejemplo, primero, se genera el archivo (el archivo SESSION LOG) y, a continuación, se copia y, sólo cuando se ha terminado de copiar, se genera y se copia el archivo COMPLETE.

-El archivo COMPLETE se envía incluso si no hay datos para enviar.

Cambiar inicio inicial de la despensa de datos:

Para cambiar la hora de inicio inicial de la despensa de datos, utilice la grdapi update_datamart.

grdapi update_datamart Name="Export:Session Log" initial_start=[valor de inicio inicial]

Por ejemplo,

Establecer el inicio inicial en la hora actual

grdapi update_datamart Name="Export:Session Log" initial_start=< >

Establecer el inicio inicial el 1 de octubre de 2016

grdapi update_datamart Name="Export:Session Log" initial_start="2016-10-01 00:00:00"

Copiar paquete de archivos

Es posible agrupar varias despensas de datos de exportación CSV. El paquete tiene la despensa de datos principal. Cada despensa de datos incluida en un paquete extrae datos en función de su propia planificación. Después de los datos extraídos principales de la despensa de datos, coloca los archivos de datos de todas las despensas de datos incluidas en el paquete en el mismo archivo tar y los envía a un servidor de destino. La despensa de datos principal tiene que tener la planificación más reciente.

Por ejemplo, el paquete incluía “Export:Full SQL”, “Export:Exception Log”, “Export:Session Log” y “Export:Session Log Ended” como despensa de datos principal.

La planificación recomendada para este paquete:

Descripción de trabajo cronString recomendado Cada hora a las:

Export:Session Log 0 45 0/1 ? * 1,2,3,4,5,6,7 00:45

Export:Session Log Ended 0 46 0/1 ? * 1,2,3,4,5,6,7 00:46

Export:Exception Log 0 25 0/1 ? * 1,2,3,4,5,6,7 00:25

Export:Full SQL 0 30 0/1 ? * 1,2,3,4,5,6,7 00:30

Crear un paquete:

grdapi datamart_copy_file_bundle action="create" bundle_name=[nombre de paquete] main_datamart_name=[nombre de despensa de datos principal del paquete]

Incluir una despensa de datos en un paquete:

grdapi datamart_copy_file_bundle action="include" bundle_name=[nombre de paquete] datamart_name=[nombre de despensa de datos]

Excluir una despensa de datos de un paquete:

grdapi datamart_copy_file_bundle action="exclude" bundle_name=[nombre de paquete] datamart_name=[nombre de despensa de datos]

Suprimir un paquete:

grdapi datamart_copy_file_bundle action="delete" bundle_name=[nombre de paquete]

Obtener la información de un paquete:

grdapi datamart_copy_file_bundle action="info" bundle_name=[nombre de paquete]

Ejemplo:

grdapi datamart_copy_file_bundle action="create" bundle_name="SFE_BUNDLE" main_datamart_name="Export:Session Log Ended"

grdapi datamart_copy_file_bundle action="include" bundle_name="SFE_BUNDLE" datamart_name="Export:Exception Log"

grdapi datamart_copy_file_bundle action="include" bundle_name="SFE_BUNDLE" datamart_name="Export:Full SQL"

grdapi datamart_copy_file_bundle action="include" bundle_name="SFE_BUNDLE" datamart_name="Export:Session Log"

> grdapi datamart_copy_file_bundle action="info" bundle_name="SFE_BUNDLE" main_datamart_name="Export:Session Log" datamart_name=""

ID=0

==========

Bundle Name: SFE_BUNDLE

==========

Main Datamart: Export:Session Log Ended

Datamarts:

Export:Full SQL

Export:Exception Log

Export:Session Log

Get_Datamart Info grdapi

get_datamart_info grdapi gets detail datamart information.

get_datamart_info datamart_name=[Nombre de despensa de datos]

Ejemplo,

grdapi get_datamart_info datamart_name="Export:Export Extraction Log"

==========

Data Mart Name: Export:Export Extraction Log

==========

Description:

Based on Report: User Defined Extraction Log

Based on Query: User Defined Extraction Log

Extract result to: File

Initial Start: 2016-04-18 09:00:00

Creation Date: 2016-12-28 18:01:24

Time Granularity: 1 HOUR

Active: true

File Name: EXP_DM_EXTRACTION_LOG

Lines per File: 500000

File Header: "UTC Offset","Name","Period Start","Period End","Run Id","Start Time","End Time","Status","File Status","Records Extracted","Details","Timestamp"

Include File Header: true

Copy File Info

Host Name: host.com

User Name: admin

Directory: /local/incoming/

Transfer Method: SCP

Bundle Name:

Bundle Main Datamart: false

Send COMPLETE File: false

Last Extraction Info

State:1

Timestamp: 2017-01-18 14:50:00

Next Period: 2017-01-18 14:00:00

Last Extracted ID: 0

Extraction Log

Timestamp: 2017-01-18 14:50:02

Extract Status: OK

Start Time: 2017-01-18 14:50:00

End Time: 2017-01-18 14:50:00

Period Start: 2017-01-18 13:00:00

Period End: 2017-01-18 14:00:00

Records Extracted: 26

Details: SCP to: host.com, User: admin, Path: /local/incoming/, File: DMv2_gibm32_EXP_DM_EXTRACTION_LOG_20170118180000.gz

Last for Period: true

File Name: /var/dump/DATAMART/EXP_DM_EXTRACTION_LOG_20170118180000.csv

Bundle Name:

File Transfer Status: Done

Comentarios

==========

La Despensa de datos de Full_SQL sólo funcionará si se han definido e instalado detalles completos o detalles enmascarados de registro.

Los valores atípicos de Despensas de datos sólo funcionarán si está habilitada la detección de valores atípicos.

Si el planificador de Despensa/s de datos se había detenido algún momento y no desea que los datos se extraigan retroactivamente, antes de volver a planificar las extracciones para ejecutar de nuevo, establezca el "Inicio inicial" correcto en la pantalla de Configuración de Despensa de datos.

Despensas de datos definidas por el usuario

La/s Despensa/s de datos definida/s por el usuario también se puede/n utilizar para transferir datos a un host de destino. La Despensa de datos tiene que ser de tipo Archivo, el Nombre de despensa de datos debe comenzar por “Export:” y el Parche de archivo empezará por “EXP_”.

Dependencias

==========

Cómo aplicar el parche:

==========

http://www-01.ibm.com/support/knowledgecenter/SSMPHH_8.2.0/com.ibm.guardium.using.doc/topics/how_to_install_patches.html?lang=en

Mandatos GuardAPI para la Despensa de datos

grdapi datamart_copy_file_bundle

Parámetros de función:

action - Serie - obligatorio - Lista de valores constantes

bundle_name - Serie - obligatorio

datamart_name - Serie

main_datamart_name - Serie

grdapi datamart_include_file_header

Parámetros de función:

includeFileHeader - Serie - obligatorio - Lista de valores constantes

Name - Serie - obligatorio

grdapi datamart_set_active

Parámetros de función:

Name - Serie - obligatorio

grdapi datamart_set_inactive

Parámetros de función:

Name - Serie - obligatorio

grdapi datamart_update_copy_file_info

Parámetros de función:

destinationHost - Serie

destinationPassword - Serie

destinationPath - Serie

destinationUser - Serie

Name - Serie - obligatorio

transferMethod - Serie - Lista de valores constantes

withCOMPLETEfile - Booleano

grdapi datamart_validate_copy_file_info

Parámetros de función:

destinationHost - Serie - obligatorio

destinationPassword - Serie - obligatorio

destinationPath - Serie - obligatorio

destinationUser - Serie - obligatorio

transferMethod - Serie - Lista de valores constantes

grdapi update_datamart

Parámetros de función:

Comment - Serie

initial_start - Fecha

Name - Serie - obligatorio

grdapi get_datamart_info

Parámetros de función:

datamart_name - Serie - obligatorio

isExtended - Booleano

Tema principal: Informes

Auditoría e informes

Guardium organiza los datos que recopila en un conjunto de dominios. Cada dominio contiene un tipo diferente de información relativa a un área específica de interés: acceso a datos, excepciones, infracciones de política, etc.

Todos los dominios y su contenido se describen en el apéndice Dominios, entidades y atributos.

Hay un creador de consultas separado para cada dominio y el acceso al mismo se controla mediante roles de seguridad. Independientemente del dominio, se utiliza la misma herramienta de creación de propósito general para crear todas las consultas. Para obtener instrucciones detalladas acerca de cómo crear consultas, consulte Consultas.

Además de un conjunto estándar de dominios, los usuarios pueden definir dominios personalizados para que contengan información que se puede subir al dispositivo de Guardium. Por ejemplo, una empresa puede tener una tabla que relacione nombres de usuario de base de datos genéricos (hr23455 o qa4872, por ejemplo) con personas reales (Paula Smith, John Doe). Una vez que se sube la tabla, los nombres reales se pueden visualizar en los informes de Guardium desde el dominio personalizado. Para obtener información más detallada sobre cómo definir y utilizar dominios personalizados, consulte la Correlación de datos externos.

Tema principal: Informes

Consultas

Utilice una de las muchas consultas predefinidas que vienen con Guardium para obtener información sobre los datos. Utilice el Creador de consultas para trabajar con consultas.

Utilice las consultas para hacer preguntas de sus datos, como, ¿cuáles son todos los clientes que actualizan una base de datos específica durante las horas de fin de semana?

Las consultas son distintas de los informes. Una consulta describe un conjunto de datos, mientras que un informe describe cómo se presentan los datos devueltos por una consulta.

Una vez que se ha completado una consulta, presente los resultados de la consulta utilizando informes. Los informes normalmente se presentan en formato tabular, pero puede personalizar el diseño como desee.

Para utilizar consultas, abra el Creador de consultas pulsando en Cumplir > Creación de informes personalizados > Creador de consultas personalizadas. Elija un dominio que consultar, seleccione una entidad principal y, a continuación, utilice la consulta como desee.

No puede modificar las consultas predefinidas, pero puede crear un clon de una consulta y modificarlo.

La entidad principal

La entidad principal que seleccione para una consulta determina lo siguiente:

- El nivel de detalle para el informe. Hay una fila de datos para cada aparición de la entidad principal incluida en el informe. La ubicación de la entidad principal dentro de la jerarquía de entidades es importante en términos de qué valores se pueden mostrar. Los atributos de las entidades que se encuentran bajo la entidad principal se pueden contar, pero no se pueden visualizar (ya que puede haber muchas apariciones para cada fila). Para elegir este nivel de detalle, seleccione el recuadro de selección Ordenar por recuento.
- El recuento total es un recuento de las instancias de la entidad principal incluida en esa fila del informe, añadidas como la última columna del informe. Para añadir o descartar la columna de recuento del informe, pulse el recuadro de selección Añadir recuento. Esto puede dar como resultado la mejora del rendimiento de la consulta/informe en algunos casos.
- Para añadir o descartar la posibilidad de visualizar una fila por valor en el informe, (lo que puede dar como resultado la mejora del rendimiento de la consulta/informe en algunos casos), pulse el recuadro de selección Añadir diferenciación. Esta selección proporciona informes condensados.
- La optimización de partición está habilitada de forma predeterminada y mejora el rendimiento de consulta con tablas de base de datos particionadas. En Guardium V10.1.2 y posterior, esta característica se puede inhabilitar deseleccionando el recuadro de selección Optimización de partición. La optimización de la partición no debe estar inhabilitada sin la dirección del soporte de IBM.
- Los campos de hora con los que se comparan los parámetros de tiempo de ejecución Period From y Period To para seleccionar las filas del informe. El Creador de consultas utiliza la entidad principal (entre otros parámetros) para determinar qué campos de hora se utilizan cuando se definen los valores Period From y Period To. Esto puede ser importante para las sesiones de larga ejecución, como por ejemplo cuando un servidor de aplicaciones mantiene abiertas las sesiones agrupadas. Cuando corresponda, se utiliza el Inicio del periodo/Final del periodo desde la entidad Periodo de acceso; en otros casos, elegirá valores de periodo de acuerdo con la entidad principal:
  - Sesión: La indicación de fecha y hora utilizada es para la última actualización que se ha realizado en la entidad de sesión
  - Inicio de sesión: Se utiliza la hora de inicio de la entidad de sesión
  - Fin de sesión: Se utiliza la hora final de la entidad de sesión
  - SQL completo: Indicación de fecha y hora desde el dominio de SQL completo; la consulta incluye filas del dominio de SQL completo aunque no estén enlazadas con valores (por ejemplo, cuando se establece Detalles completos de registro, no hay valores)
  - Valores de SQL completo: Indicación de fecha y hora del dominio de SQL completo; la consulta incluye filas sólo si tienen valores del dominio de SQL completo incluso si no están enlazados con el dominio de Campo
  - Valores de campo SQL: Indicación de fecha y hora del dominio de SQL completo; la consulta sólo incluye filas si tienen valores del dominio de SQL completo y si están enlazadas con el dominio de Campo
- En la pantalla Entidad principal se encuentra la selección Ejecutar en dos etapas.

  Utilice esta selección para la ejecución en dos etapas del informe Tareas de auditoría de tipo.

  Esto sólo se aplica a los informes sobre consultas en tablas específicas. Este mecanismo de dos etapas se aplica a las consultas en ejecución como procesos de auditoría con columnas y condiciones sólo en las entidades siguientes: Acceso (cliente/servidor), Sesión, Periodo de acceso, Construcción (SQL), Objeto y Sentencia (mandato).

  Este mecanismo de dos fases no se utiliza si la consulta contiene una condición con el operador `Like Group` o cualquier otro operador relacionado con alias (como por ejemplo `In Aliases Group`) o la condición utiliza Having.

  Además de utilizar el creador de consultas, cada consulta se puede establecer de forma que se ejecute en dos etapas. De forma predeterminada, las consultas se ejecutan utilizando el método anterior. Para que una consulta se ejecute en dos etapas, se debe establecer un distintivo en el creador de consultas. Además, este

método de ejecución de consultas se puede inhabilitar (en todo el sistema) para hacer que todas las tareas de auditoría utilicen el método antiguo creando el archivo: /var/log/guard/DontRunInTwoStages. La existencia de este archivo indica que NO se debe utilizar el nuevo método de dos etapas.
Nota: Los campos que contienen tuplas (campos combinados) en la Ejecución en dos etapas no están soportados en este release.

Nota: Nota: La lista desplegable Entidad principal sólo incluye las entidades primarias. Sin embargo, el acceso a entidades secundarias (por ejemplo, Inicio de sesión y Final de sesión) se puede realizar a través de su entidad primaria correspondiente (por ejemplo, Sesión para inicio de sesión y Fin de sesión).

Clasificación

De forma predeterminada, los datos de consulta se clasifican en orden ascendente por valor de atributo, con las claves de ordenación ordenadas según aparecen los atributos en la consulta. Los alias se ignoran para fines de clasificación. Los valores de datos reales siempre se utilizan para la clasificación. Los atributos para los que los valores se calculan mediante la consulta (Recuento, Mín, Máx o Media) no se pueden clasificar.

Para cambiar el orden de clasificación predeterminado:

1. Marque el recuadro de selección Ordenar por.
2. Escriba un número para Clasificación de ordenación (1 es la tecla de ordenación mayor).
3. Opcionalmente, seleccione el recuadro de selección Descend para clasificar los valores de dicho atributo en secuencia descendente.

La última columna de un informe tabular es un recuento de las apariciones de la entidad principales. Para ordenar este recuento en secuencia descendente (es decir, en otras palabras, listar en primer lugar las apariciones de número más alto), marque el recuadro de selección Ordenado por apariciones.

Indicaciones de fecha y hora

Una indicación de fecha y hora (t minúscula) es un tipo de datos que contiene un valor de fecha y hora combinado, que cuando se imprime se visualiza en el formato aaaa-mm-dd hh:mm:ss (por ejemplo, 2012-07-17 15:40:25). Al crear o editar una consulta, la mayoría de los atributos con un tipo de datos de indicación de fecha y hora se muestran con un icono de reloj en el panel Lista de entidades.

Una indicación de fecha y hora (T mayúscula) es un atributo definido en muchos tipos de entidades, que contiene la hora en que la entidad se actualizó por última vez. Para muchos atributos de indicación de fecha y hora, puede imprimir los componentes de fecha, hora, día de la semana o año por separado, haciendo referencia a atributos adicionales de indicación de fecha y hora (Fecha, Hora de día de la semana o Año).

- Utilización del Creador de consultas
  Utilice el Creador de consultas para crear o modificar consultas. Especifique el dominio que desea consultar, elija una entidad principal y, a continuación, utilice el Creador de consultas para definir o modificar una consulta.
- Condiciones de consulta
  Utilice los operadores AND, OR y HAVING con paréntesis para crear condiciones de consulta.

Tema principal: Informes

Utilización del Creador de consultas

Utilice el Creador de consultas para crear o modificar consultas. Especifique el dominio que desea consultar, elija una entidad principal y, a continuación, utilice el Creador de consultas para definir o modificar una consulta.

1. Abra el Creador de consultas pulsando Cumplir > Creación de informes personalizados > Creador de consultas personalizadas.
2. Determine el dominio que desea consultar. Seleccione un elemento en el menú Buscador de dominios y pulse Buscar, o pulse Nuevo para crear un dominio personalizado.
3. Elija una consulta existente utilizando los menús de filtro en el Buscador de consultas, o pulse Nuevo para crear una consulta nueva.
4. Hay tres componentes principales en la pantalla Creador de consultas:
   - El panel Lista de entidades identifica todas las entidades y atributos contenidos en el dominio. Las entidades se representan como carpetas, y los atributos son los elementos dentro de las carpetas. Pulse una carpeta de entidad para mostrar sus atributos, o pulse otra vez para ocultarlos. Para obtener una descripción de todas las entidades y atributos, consulte Entidades y atributos en la información de Dominios, entidades y atributos.
   - El panel Campos de consulta lista todos los campos a los que se debe acceder, lo que se debe visualizar para ese campo (su valor, un recuento, mínimo, máximo o promedio) y el orden de clasificación. Para obtener más información sobre cómo utilizar este panel, consulte *Visión general de campos de consulta*.
   - El panel Condiciones de consulta especifica las condiciones para seleccionar estos campos (por ejemplo, `where VERB = UPDATE`). Para obtener más información sobre el uso de este panel, consulte *Visión general de condiciones de consulta*.

Creación de una consulta

1. Abra el Creador de consultas para el dominio apropiado.
2. Pulse Nuevo para abrir el panel Nueva consulta – Detalles generales.
3. Escriba un nombre de consulta exclusivo en el recuadro Nombre de consulta. No incluya caracteres de apóstrofo en el nombre de consulta.
4. Seleccione la entidad principal para la consulta en la lista Entidad principal. Recuerde que la entidad principal controla el nivel de detalle que está disponible para la consulta y que no se puede cambiar. Básicamente, cada fila de datos devuelta por la consulta representará una instancia exclusiva de la entidad principal y un recuento de apariciones para dicha instancia.
5. Pulse Siguiente. La nueva consulta se abre en el panel Creador de consultas. Para completar la definición, consulte uno de los temas siguientes:
   - Visión general del Creador de consultas
   - Modificar una consulta

Modificación de una consulta

No puede modificar las consultas predefinidas de Guardium, pero puede clonar una consulta y modificar el clon según sea necesario.

1. Elija un dominio y una entidad principal para abrir el Creador de consultas para la consulta que desea modificar.
2. Pulse Clonar, especifique un nombre nuevo para la consulta (no se permiten los apóstrofos) y pulse Guardar.
3. Consulte el tema Visión general del creador de consultas para modificar cualquier componente de la definición de consulta.

Eliminación de una consulta

No puede eliminar una consulta que está siendo utilizada por algún otro componente. Para suprimir una consulta de este tipo, primero debe suprimir todos los componentes que la utilicen (por ejemplo, informes o alertas de correlación). Al intentar suprimir una consulta, se listarán los informes y las alertas de correlación dependientes de la consulta.

1. Elija un dominio y una consulta para abrir el Creador de consultas para la consulta que desea suprimir.
2. Pulse Suprimir.

Visión general de Campos de consulta

El panel Campos de consulta lista las columnas de datos que la consulta debe devolver.

Los menús Modalidad de campo indican qué se debe imprimir para el campo: su Valor, su Cuenta (número de valores distintos), Mín, Máx, Promedio (AVG) o Suma para la fila. La selección de Valor no está disponible para atributos de entidades mayores que la entidad principal en la jerarquía de entidad para el dominio.

Hay dos formas de añadir un campo en el panel Campos de consulta:

- Método de menú emergente:
  1. En la Lista de entidades, pulse el campo que se va a añadir.
  2. Seleccione Añadir campo en el menú emergente.
- Método de arrastrar y soltar:
  1. En la Lista de entidades, pulse en el icono del nombre de campo (no en el propio nombre de campo), arrastre el icono al panel Campos de consulta y suéltelo.

Cuando se añade un campo, éste se añadirá al final de la lista.

Para mover un campo hacia arriba o hacia abajo en el panel Campos de consulta, marque el recuadro de selección del campo y pulse los iconos Arriba o Abajo para mover el campo una fila hacia arriba o hacia abajo.

Una advertencia sobre los atributos de SQL completo en las consultas

Tenga cuidado al utilizar el atributo de SQL completo en una consulta. Puede producir informes excesivamente grandes, porque cada valor distinto del atributo (la serie de consultas SQL completa en este caso) se devolverá en una fila independiente.

Por otro lado, es posible que el informe no contenga ninguna información, o muchas columnas en blanco donde se esperan series SQL completas. Guardium captura SQL completo sólo cuando se lo indican las reglas de política, y es posible que las reglas no se hayan desencadenado durante el periodo del informe.

No confunda el atributo de SQL completo con la posibilidad de detallar más hasta el SQL para la mayoría de las consultas del dominio de Acceso de datos que tengan algo que ver con las solicitudes de SQL.

Grupos de tipos distintos de los tipos definidos en el atributo

La validación en el tipo de grupo suele ser restrictiva. Consulte Visión general de grupos para ver ejemplos sobre los tipos de grupo. Mediante el uso de Condiciones de consulta, el Creador de consultas, se permite un grupo de tipos distintos del tipo definido para el atributo en la condición de grupo. Estas opciones adicionales son sólo para los operadores IN GROUP e IN DYNAMIC GROUP. La selección de tipos que no sean el tipo definido para la condición se realiza en el parámetro Tiempo de ejecución del informe tabular.

1. Cree un grupo en el Creador de grupos pulsando Configuración > Herramientas y Vistas > Creador de grupos. Especifique un Nombre de grupo y elija OBJECTS para Tipo de grupo.
2. Cree un Informe de acceso en el Creador de informes pulsando Configuración > Informes > Creador de informes.
3. Especifique un nombre de consulta y pulse en la carpeta OBJECT de la Lista de entidades para poder ver más opciones.
4. Resalte Nombre de objeto y pulse una vez para obtener la opción ADD CONDITION. Pulse Añadir condición de forma que se añada una línea a la sección Condiciones de consulta en el cuerpo principal de la pantalla de menú.
5. Vaya a la selección desplegable junto al atributo Nombre de objeto y elija, en la columna Operador, IN GROUP o IN DYNAMIC GROUP. En la segunda selección desplegable (columna Parámetro de tiempo de ejecución), elija el grupo que ha creado en el paso 1.
6. Guarde el trabajo. Pulse Generar tabular y, a continuación, pulse Añadir a mis informes nuevos.
7. Vaya al separador Mis informes nuevos y resalte el informe que ha creado.
8. Pulse Personalizar junto al nombre de informe. Se abrirá un separador denominado Personalizar portlet (Parámetros de tiempo de ejecución).
9. Abra la selección desplegable y los grupos del tipo correspondiente a la entidad que se está probando aparecerán al principio de la lista, a continuación una línea de guión doble y, a continuación, el resto de los grupos. Aquí es donde se pueden seleccionar distintos grupos.
10. Guarde el trabajo pulsando Actualizar.

Tabla 1. Botones

Botones	Pasos
Suprimir	1. Seleccione la consulta que se va a suprimir. 2. Pulse Suprimir.
Clonar	1. Seleccione la consulta que se va a clonar. 2. Pulse Clonar. 3. Especifique un nombre nuevo para la consulta clonada.
Roles	La asignación de roles a informes mientras está en el Creador de consultas sólo asigna el rol a la Consulta, no el informe. Asigne roles a los informes en el Creador de informes. Consulte Informes.
Guardar	Pulse Guardar cuando haya terminado todas las tareas necesarias en la pantalla de menú.
Atrás	Retroceda entre pantallas de menú de una tarea o función de Guardium de pantalla múltiple utilizando el botón Atrás. La flecha atrás en el navegador web no funciona para la navegación entre pantallas de menú.
Establecer como despensa de datos	Una despensa de datos es un tipo de almacén de datos. Un almacén de datos agrega y organiza los datos de una forma genérica que se pueden utilizar posteriormente para informes y análisis.

Tema principal: Consultas
Conceptos relacionados:

Condiciones de consulta

Utilice los operadores AND, OR y HAVING con paréntesis para crear condiciones de consulta.

Los operadores AND, OR y HAVING están ubicados en la barra de título Condiciones de consulta en el Creador de consultas.

Seleccione en la Lista de entidades y utilice los operadores para crear condiciones de consulta como parte de su consulta.

Uso de los operadores AND y OR:

- Los operadores AND tienen prioridad sobre los operadores OR.
- Añada un operador AND o un operador OR al final o en la mitad de la lista de condiciones utilizando el menú de añadir condición o arrastre y suelte el icono del atributo. Seleccione y elimine condiciones pulsando Suprimir. Guarde la consulta. Si la consulta SQL generada no es válida, la consulta no se guardará y se generará un mensaje de error.

Utilización de paréntesis:

- Todas las condiciones son independientes. Agrupe las condiciones mediante la adición de los paréntesis izquierdo y derecho alrededor de las condiciones. Utilice corchetes en condiciones de consulta complicadas.
- Cuando se selecciona una condición, al pulsar el botón de paréntesis izquierdo se añade una condición de paréntesis izquierdo antes de la primera condición seleccionada. Si se pulsa el botón de paréntesis derecho se añadirá una condición de paréntesis derecho después de la primera condición seleccionada. Si no hay ninguna condición seleccionada, pulsar los botones de paréntesis no tendrá ningún efecto.
- Cuando se crea una condición de consulta que utiliza paréntesis, los paréntesis aparecen en la IU ANTES del operador, pero se aplican DESPUÉS del operador. Por ejemplo, una condición de consulta se visualiza como *this (AND that OR another)*. Sin embargo, la lógica real es *this AND (that OR another)*.

Escape de caracteres de barra inclinada invertida (\): Para escapar correctamente un carácter de barra inclinada invertida para su uso en una condición de consulta, utilice cuatro caracteres de barra inclinada. Por ejemplo, para especificar `dominio\usuario`, debe especificar `dominio\\\\usuario`.

Hay dos partes en el panel de visualización de condición: una empieza con una condición WHERE y otra empieza con una condición HAVING.

En la parte HAVING, el campo de agregación tiene opciones: Recuento, Mín, Máx y AVG. La opción SUM también se aplica a determinadas entidades con ID en el nombre (ID de sesión, ID global, ID de SQL completo, ID de instancia). Si el botón HAVING no está seleccionado, la condición se insertará en la parte WHERE con el campo agregado como serie vacía. Si el botón HAVING está seleccionado, la condición se inserta en la parte HAVING y el campo agregado tiene opciones. Después de añadir o eliminar una condición, la opción de condición se actualizará. Al pulsar SAVE, se generará un SQL. El SQL se valida antes de guardarlo. Si ha fallado la validación (por ejemplo, error de sintaxis), se genera un mensaje de error de alerta y se pone una descripción de error más detallada en el registro. Si se añade una condición en la parte incorrecta, (por ejemplo, se ha establecido el botón HAVING y el icono de atributo se ha descartado en la parte WHERE, o viceversa) se genera un mensaje de alerta no coincidente. Si la condición seleccionada está en la parte WHERE, pero está establecido el botón HAVING, la condición de adición falla porque el valor no coincide.

Los atributos Acceso total, SQL fallidos y SQL satisfactorios sólo se pueden añadir bajo una cláusula HAVING (no la cláusula WHERE).

Las consultas permitidas deben tener una columna de indicación de fecha y hora y, como mínimo, una columna con Modalidad=Recuento O el conjunto de distintivos de recuento (o ambos). La columna de consulta que debe evaluarse mediante la consulta debe ser una de las columnas con Modalidad=Recuento O la columna de acceso total (si se ha establecido el distintivo de recuento).

Añadir o eliminar una condición de consulta

1. Para eliminar una condición de consulta, marque el recuadro de selección en la fila para dicha condición, y pulse el botón X (Suprimir elemento marcado) en la barra de título Condiciones de consulta.
2. Para añadir una condición, cree una fila en la lista Condiciones de consulta para el campo adecuado desde el panel Lista de entidades.

   Para añadir una condición AND, seleccione el botón de selección AND en la barra de título Condiciones de consulta y realice una de las acciones siguientes:

   - Seleccione una entidad en el panel Lista de entidades y seleccione Añadir condición en el menú emergente.
   - Arrastre el icono de campo desde el panel Lista de entidades y suéltelo en el panel Condiciones de consulta.

   Para añadir una condición OR, seleccione el botón de selección OR en la barra de título Condiciones de consulta y realice una de las acciones siguientes:

   - Arrastre el icono de campo desde el panel Lista de entidades y suéltelo hasta el principio de la condición para la que es una condición OR.
   - Marque el recuadro de selección para la condición a la que desea añadir la condición OR, pulse el campo en el panel Lista de entidades y, a continuación, seleccione Añadir condición en el menú emergente.

3. *Opcional*: Utilice el menú desplegable Agregado para seleccionar un agregado del atributo que se utilizará para la condición de consulta: Recuento, Mín (valor mínimo), Máx (valor máximo) o AVG (valor promedio). Se aplican las restricciones, de la siguiente manera:
   - No puede utilizar un agregado en una condición OR.
   - No puede añadir una condición OR a una condición que contenga un agregado.
4. Seleccione el operador para la condición nueva en la lista. No todos los tipos de atributo tienen el mismo conjunto de operadores disponibles. Por ejemplo, los atributos que no se pueden asociar a grupos no tendrán ninguna de las opciones de grupo (IN GROUP, LIKE GROUP). Sin embargo, cuando se añaden tuplas (varios atributos que se combinan para formar un único grupo) como condición de una consulta, todos los operadores para la nueva condición están disponibles para su selección.

Tabla 1. Operador para Condición nueva

Operador	Descripción
<	Menor que
< =	Menor o igual a
< >	No igual a

Operador	Descripción
=	Igual a
>	Mayor que
> =	Mayor o igual a
CATEGORIZED AS	Miembro de un grupo perteneciente a la categoría seleccionada en la lista desplegable, que aparece cuando se selecciona un operador de grupo.
CLASSIFIED AS	Miembro de un grupo perteneciente a la clasificación seleccionada en la lista desplegable, que aparece cuando se selecciona un operador de grupo.
IN DYNAMIC GROUP	Miembro de un grupo que se selecciona en la lista desplegable de la columna de parámetros de tiempo de ejecución, que aparece cuando se selecciona un operador de grupo.
IN GROUP	Miembro del grupo que se ha seleccionado en la lista desplegable de la columna de parámetros de tiempo de ejecución, que aparece cuando se selecciona un operador de grupo. IN GROUP o IN ALIASES GROUP no se pueden utilizar a la vez.
IN DYNAMIC ALIASES GROUP	El operador trabaja en un grupo del mismo tipo que IN DYNAMIC GROUP, sin embargo, asume que los miembros del grupo son alias.
IN ALIASES GROUP	El operador trabaja en un grupo del mismo tipo que IN GROUP, sin embargo, asume que los miembros del grupo son alias. Tenga en cuenta que los operadores IN GROUP/IN ALIASES GROUP esperan que el grupo contenga valores reales o alias, respectivamente. Un alias proporciona un sinónimo que se sustituye por un valor almacenado de un tipo de atributo específico. Se utiliza normalmente para mostrar un nombre descriptivo o fácil de usar para un valor de datos. Por ejemplo, es posible que el Servidor financiero se haya definido como un alias para la dirección IP 192.168.2.18.
IS NOT NULL	El valor de atributo existe, pero puede estar en blanco o no ser imprimible
IS NULL	Atributo vacío
IN PERIOD	Sólo para una indicación de fecha y hora, está dentro del periodo de tiempo seleccionado
LIKE	
LIKE GROUP	Coincide con un valor similar que se ha especificado en los recuadros. Un valor similar utiliza el signo de porcentaje como un carácter comodín y coincide con todo o parte del valor. Los caracteres alfabéticos no distinguen entre mayúsculas y minúsculas. Por ejemplo, %tea% coincidiría con tea, TeA, tEam, steam. Si no se incluye ningún signo de porcentaje, la operación de comparación es una operación de igualdad (=).
NOT IN DYNAMIC GROUP	No es igual a ningún miembro de un grupo, que se selecciona en la lista desplegable de la columna de parámetros de tiempo de ejecución, que aparece cuando se selecciona un operador de grupo.
NOT IN DYNAMIC ALIASES GROUP	El operador trabaja en un grupo del mismo tipo que NOT IN DYNAMIC GROUP, sin embargo, asume que los miembros de ese grupo son alias.
NOT IN GROUP	No es igual a ningún miembro del grupo especificado, que se selecciona en la lista desplegable de la columna de parámetros de tiempo de ejecución, que aparece cuando se selecciona un operador de grupo.
NOT IN ALIASES GROUP	El operador trabaja en un grupo del mismo tipo que NOT IN GROUP, sin embargo, presupone que los miembros de ese grupo son alias.
NOT IN PERIOD	Sólo para una indicación de fecha y hora, no dentro del periodo de tiempo seleccionado
NOT LIKE	No es igual que el valor especificado (consulte la descripción de LIKE)
NOT LIKE GROUP	No es igual que el valor que se ha especificado en LIKE GROUP
NOT REGEXP	No coincide con la expresión regular especificada
REGEXP	Coincide con la expresión regular especificada. Para obtener información detallada acerca de cómo utilizar expresiones regulares, consulte Expresiones regulares.

Nota: Hay cuatro palabras especiales que no están permitidas como nombre de parámetro: usuario; grupo; rol; página.

Se producirá un error si se realiza un intento de guardar una consulta con cualquiera de estas palabras en el parámetro. Hay dos tipos de condiciones donde esto se aplica:

- Cuando cree una condición de consulta con un operador como =, <, LIKE, etc, y a continuación, seleccione Parámetro. Este campo no permite las palabras especiales.
- Cuando se crea una condición de consulta con un operador de tipo DYNAMIC GROUP (IN, NOT IN, IN ALIAS, etc), este campo no permite las palabras especiales.

5. Para un operador de grupo, seleccione un grupo de la lista.

Para la mayoría del resto de los operadores, debe facilitar un valor para la condición, o indicar que un valor de parámetro de tiempo de ejecución (que no contiene signos de exclamación) se proporciona más tarde (cuando se ejecuta la consulta). En estos casos, aparece un menú desplegable con tres opciones. Realice una de las siguientes acciones:

- Seleccione Valor y especifique un valor exacto en el recuadro.
- Seleccione Parámetro y especifique un nombre para el parámetro de tiempo de ejecución (el nombre no debe contener espacios).
- Seleccione Atributo y seleccione otro atributo para que coincida con el atributo seleccionado (por ejemplo, esto se puede utilizar para probar el tráfico local haciendo coincidir las direcciones IP de servidor y cliente).

Hay un icono Añadir expresión junto a las selecciones de Valor, Parámetro, Atributo. Utilice este icono para especificar condiciones de consulta, incluida la serie definida por el usuario y expresiones matemáticas.

Utilice esta característica cuando el usuario necesite añadir una condición que no esté basada en todo el contenido del atributo tal cual, sino en parte del atributo, una función del atributo o una función que combine más de un atributo.

Un ejemplo sería: `INSTR(:attribute, '150.1') = 5`, que devuelve todas las instancias de IP de cliente que coinciden con los 5 caracteres listados. Escriba el carácter 5 en el recuadro de entrada situado junto al icono Añadir expresión. Escriba la expresión `INSTR(:attribute, '150.1')` en la ventana Crear expresión independiente. Pruebe la validez de la expresión en la ventana Crear expresión. Otro ejemplo es: `LENGTH(:attribute) >= 40`, que devuelve la longitud de cualquier sentencia de SQL de más de 40 caracteres. La expresión puede contener o no referencias al atributo real y también puede contener referencias a otros atributos.

6. Cuando haya terminado de añadir todas las condiciones, recuerde que debe guardar la definición.

Crear expresión en condición de consulta

Hay un icono Añadir expresión junto a las selecciones de Valor, Parámetro, Atributo. Utilice este icono para especificar condiciones de consulta, incluida la serie definida por el usuario y expresiones matemáticas.

Utilice esta característica cuando el usuario necesite añadir una condición que no esté basada en todo el contenido del atributo tal cual, sino en parte del atributo, una función del atributo o una función que combine más de un atributo.

Un ejemplo:

Devolver la ubicación de la serie `150.1`, a partir del valor 192.150.1.x., donde la serie `150.1` se encuentra en el quinto carácter del valor. La serie `150.1` representa todas las instancias de IP de cliente que coinciden con los 5 caracteres listados.

Cuando la función se ejecuta en el campo Expresión, devuelve un valor, y ese valor debe estar en el recuadro de entrada.

Utilice la función, `INSTR(:attribute, '150.1')` con un valor "5" en el recuadro de entrada situado junto al icono Añadir expresión para devolver los registros con `150.1` en la quinta ubicación.

Si la función es `INSTR(:attribute, '150.1') = 5`, se convertirá en una frase booleana, y los únicos valores en el recuadro de entrada serán 0 o 1.

Escriba la expresión `INSTR(:attribute, '150.1')` en la ventana Crear expresión independiente.

Pruebe la validez de la expresión en la ventana Crear expresión.

Otro ejemplo: `LENGTH(:attribute) >= 40`, que devuelve la longitud de cualquier sentencia de SQL de más de 40 caracteres. La expresión puede contener o no referencias al atributo real y también puede contener referencias a otros atributos.

Tema principal: Consultas

Dominios, entidades y atributos

Un dominio proporciona una vista de los datos que Guardium almacena.

Cada dominio contiene un conjunto de datos relacionados con una finalidad o función específica (acceso a datos, excepciones, infracciones de política, etc.). Para obtener una descripción de todos los dominios, consulte Dominios.

Cada dominio contiene una o más entidades. Una entidad es un conjunto de atributos relacionados y un atributo es básicamente un valor de campo. Para obtener una descripción de todas las entidades y atributos, consulte la sección de Entidades y atributos.

Una consulta de Guardium sólo devuelve datos de un dominio. Cuando se define la consulta, una entidad dentro de dicho dominio se designa como la entidad principal de la consulta. Cada fila de datos que la consulta devuelve contendrá un recuento de las apariciones de la entidad principal que coincida con los valores devueltos para los atributos seleccionados, dentro del periodo de tiempo solicitado. Esto permite la creación de informes bidimensionales a partir de entidades que no tienen una relación de uno a uno.

Hay un creador de consultas separado para cada dominio y el acceso al mismo se controla mediante roles de seguridad. Por lo tanto, cada rol de Guardium tiene normalmente acceso a un subconjunto de dominios, dependiendo de la función de dicho rol dentro de la empresa. Los usuarios con el rol de administrador de Guardium habitualmente tienen acceso a todos los dominios de informes.

Algunos dominios solo están disponibles cuando determinados componentes opcionales están instalados (CAS o Clasificación, por ejemplo). También hay disponible información de informes de otros dominios pertenecientes al dispositivo Guardium (actividad de archivado, por ejemplo) que está únicamente disponible de forma predeterminada para los usuarios con el rol de administrador de Guardium).

Algunos de los atributos descritos en este apéndice están disponibles únicamente para los usuarios con el rol de administrador. Están etiquetados con: Reservado únicamente para la utilización por parte del rol de administrador.

Para los usuarios que no tienen el rol de administrador, estos atributos no estarán disponibles en el creador de consultas.

De forma similar, no todos los atributos están disponibles para todos los protocolos de base de datos. Cuando se utiliza un creador de consultas, si observa que una entidad o atributo descrito en la documentación no aparece en el panel de Entidades, dicha entidad o atributo no está disponible para el tipo de base de datos seleccionado.

Consulte los temas siguientes:

- Dominios
- Entidades y atributos
- Creación de consultas

- Dominios
  En la tabla siguiente se describen los creadores de consultas y los dominios asociados que se proporcionan con el sistema Guardium. Es posible que su empresa haya definido dominios personalizados adicionales.
- Dominios personalizados
  Los dominios personalizados permiten dominios definidos por el usuario y pueden definir cualquier tabla de datos que se haya cargado en el dispositivo.
- Entidades y atributos
  Este tema contiene una descripción de los atributos contenidos en cada entidad.
- Informes de titularidad de base de datos
  Puede utilizar informes de titularidad de base de datos para verificar que los usuarios sólo tienen acceso a los datos adecuados. El sistema Guardium incluye

informes predefinidos de titularidad de base de datos para varios tipos de bases de datos.

Tema principal: Informes

Dominios

En la tabla siguiente se describen los creadores de consultas y los dominios asociados que se proporcionan con el sistema Guardium. Es posible que su empresa haya definido dominios personalizados adicionales.

Cada dominio contiene un conjunto de datos relacionados con una finalidad o función específica (acceso a datos, excepciones, infracciones de política, etc.). Para obtener una descripción de todos los dominios, consulte Dominios.

Cada dominio contiene una o más entidades. Una entidad es un conjunto de atributos relacionados y un atributo es básicamente un valor de campo. Para obtener una descripción de todas las entidades y atributos, consulte la sección de Entidades y atributos.

Una consulta de Guardium sólo devuelve datos de un dominio. Cuando se define la consulta, una entidad dentro de dicho dominio se designa como la entidad principal de la consulta. Cada fila de datos que la consulta devuelve contendrá un recuento de las apariciones de la entidad principal que coincida con los valores devueltos para los atributos seleccionados, dentro del periodo de tiempo solicitado. Esto permite la creación de informes bidimensionales a partir de entidades que no tienen una relación de uno a uno.

Hay un creador de consultas separado para cada dominio y el acceso al mismo se controla mediante roles de seguridad. Por lo tanto, cada rol de Guardium tiene normalmente acceso a un subconjunto de dominios, dependiendo de la función de dicho rol dentro de la empresa. Los usuarios con el rol de administrador de Guardium habitualmente tienen acceso a todos los dominios de informes.

Algunos dominios solo están disponibles cuando determinados componentes opcionales están instalados (CAS o Clasificación, por ejemplo). También hay disponible información de informes de otros dominios pertenecientes al dispositivo Guardium (actividad de archivado, por ejemplo) que está únicamente disponible de forma predeterminada para los usuarios con el rol de administrador de Guardium).

Algunos de los atributos descritos en este apéndice están disponibles únicamente para los usuarios con el rol de administrador. Están etiquetados con: Reservado únicamente para la utilización por parte del rol de administrador.

Para los usuarios que no tienen el rol de administrador, estos atributos no estarán disponibles en el creador de consultas.

De forma similar, no todos los atributos están disponibles para todos los protocolos de base de datos. Cuando se utiliza un creador de consultas, si observa que una entidad o atributo descrito en la documentación no aparece en el panel de Entidades, dicha entidad o atributo no está disponible para el tipo de base de datos seleccionado.

Consulte los temas siguientes:

- Dominios
- Entidades y atributos
- Creación de consultas

El acceso al creador de consultas para cada dominio se controla mediante roles de seguridad, de modo que cada rol de usuario tiene normalmente acceso a un conjunto independiente de dominios. Algunos dominios solo están disponibles cuando determinados componentes opcionales están instalados (por ejemplo, CAS).

En el portal de administración predeterminado, todos los creadores de consultas se pueden abrir desde el menú de separadores Herramientas > Creación de informes. En el portal de usuario predeterminado, muchos creadores de consultas se pueden abrir desde la aplicación de Creación de informes personalizados: Supervisar/Auditar > Crear informes.

A continuación de una breve descripción del dominio, la columna Descripción lista el rol de seguridad predeterminado asignado a cada dominio e indica cómo acceder al dominio desde el portal de usuario predeterminado (si está disponible).

Tabla 1. Dominios

Creador de consultas (dominio)	**Descripción**
Política de acceso (Política de acceso)	Utilice este dominio para realizar un seguimiento de todas las políticas disponibles en el sistema. Es similar al dominio de Políticas instaladas para realizar un seguimiento de todas las políticas instaladas en el sistema. Roles: todos. Portal de usuario: no disponible.
Acceso (INFO DE REGISTRADOR)	Todos los datos relacionados de cliente/servidor, sesión, SQL y periodos de acceso. Se trata de los datos recopilados por los motores de inspección cada vez que se envía una solicitud a un servidor que se está supervisando. Roles: todos. Portal de usuario: Supervisar/Auditar > Crear informes > Seguir acceso de datos
Agregación/Archivado (AGREGACIÓN/EXPORTACIÓN/IMPORTACION)	Actividad de agregación y archivado, incluida fecha, hora y estado de cada operación (archivado, envío, depuración, etc.). Roles: administrador. Portal de usuario: No disponible.
Alerta (ALERTA)	Todas las alertas generadas y enviadas por Guardium. Roles: todos. Portal de usuario: Supervisar/Auditar > Crear informes > Seguir alertas enviadas
Aplicación (Datos de aplicación)	Datos de conexión, sesión y aplicación registrados para aplicaciones especiales que no sean Guardium (por ejemplo, SAP y SAP). Roles: administrador. Portal de usuario: No disponible.
Proceso de auditoría (SEGUIMIENTO DE AUDITORÍA)	La ejecución de procesos de auditoría y la distribución de resultados. Roles: todos. Portal de usuario: Supervisar/Auditar > Crear informes > Creador de proceso de auditoría

Creador de consultas (dominio)	Descripción
Descubrimiento automático (DESCUBRIMIENTO BD AUTODETECCIÓN)	Actividad de descubrimiento automático de base de datos, incluidos todos los procesos que se han ejecutado y los hosts y puertos descubiertos. Roles: todos. Portal de usuario: Descubrir > Descubrimiento de BD > Creador de consultas de descubrimiento automático
Cambios de CAS (Cambios de CAS)	Todos los cambios detectados por CAS, incluidos los datos cambiados registrados. Roles: cas. Portal de usuario: No disponible.
Configuración de CAS (Configuración de CAS)	Configuraciones de instancias, describiendo la utilización de plantillas en hosts específicos. Roles: cas. Portal de usuario: No disponible.
Historial de hosts de CAS (Historial de hosts de CAS)	Historial de cambios de CAS aplicados a hosts de agente de CAS. Roles: cas. Portal de usuario: No disponible.
Plantillas de CAS (Plantillas de CAS)	Informa sobre el contenido de las plantillas de CAS (que definen los elementos que se deben supervisar). Roles: cas. Portal de usuario: No disponible.
Resultados de clasificador (Proceso de clasificación)	Informa sobre ejecuciones y resultados del proceso del clasificador. Roles: administrador. Portal de usuario: No disponible.
Comentarios (COMENTARIO)	Comentarios definidos por el usuario para los distintos componentes de Guardium. Roles: todos. Portal de usuario: Supervisar/Auditar > Crear informes > Creador de comentarios
Creador de dominios personalizados	Se han definido dominios personalizados para subir productos y tablas utilizados habitualmente. Consulte Tabla personalizada puesto que un dominio personalizado contiene una o varias tablas personalizadas. Si contiene varias tablas, debe definir las relaciones entre las tablas al definir el dominio personalizado.
Creador de consultas personalizadas	Los dominios definidos por el usuario definen tablas de datos que se suben al dispositivo Guardium. Roles: todos. Portal de usuario: Supervisar/Auditar > Crear informes > Creador de consultas personalizadas
Creador de tablas personalizadas	Una tabla personalizada contiene uno o más atributos que el usuario desea tener disponibles en el dispositivo Guardium. Por ejemplo, es posible que tenga una tabla de base de datos existente que relacione nombres de usuario codificados con nombres reales. En el tráfico de red, solo se verán los nombres codificados. Al definir una tabla personalizada en el dispositivo Guardium y al subir datos para dicha tabla desde la tabla existente, podrá relacionar los nombres reales y los codificados.
Usuarios predeterminados de BD habilitados	Escaneo sin credenciales: Proceso para escanear una lista de bases de datos y comprobar si los usuarios predeterminados están habilitados. Los usuarios predeterminados, así como la lista de servidores que se deben escanear, se proporcionan como parámetros para la API. Se proporciona un grupo predeterminado para cada tipo de base de datos con los usuarios y las contraseñas predeterminados creados por la base de datos en cada instalación. Los clientes pueden añadir/eliminar de dicha lista. Los grupos son de tipo Usuario BD/Contraseña BD y los nombres de los grupos predeterminados son: Usuarios predeterminados de ORACLE; Usuarios predeterminados de DB2; Usuarios predeterminados de SYBASE; Usuarios predeterminados de MS SQL SERVER; Usuarios predeterminados de INFORMIX; Usuarios predeterminados de MYSQL; Usuarios predeterminados de TERADATA; Usuarios predeterminados de IBM® ISERIES; Usuarios predeterminados de POSTGRESQL; Usuarios predeterminados de NETEZZA
Instancias descubiertas (Instancias descubiertas)	Instancias descubiertas por GIM Roles: todos Portal de usuario: Supervisar/Auditar > Crear informes > Instancia descubierta
Uso de almacenamiento intermedio de empresa	Muestra el uso de almacenamiento intermedio de sniffer de todas las unidades gestionadas. Roles: ninguno. Portal de usuario: No disponible.
Excepciones (consulte la nota al final de la tabla) (EXCEPCIONES DE REGISTRADOR)	Todas las excepciones y datos relacionados con las excepciones. Se trata de las excepciones SQL enviadas desde un servidor de bases de datos y recopiladas por los motores de inspección, así como las excepciones generadas por el propio Guardium. Roles: todos. Portal de usuario: Supervisar/Auditar > Crear informes > Seguir excepciones
Flat Log (Flat Log)	Actividad de procesos Flat Log. Roles: ninguno. Portal de usuario: Supervisar/Auditar > Crear informes > Creador de Flat Log
Sucesos de GIM (Sucesos de GIM)	Guardium Installation Manager Roles: todos Portal de usuario: Supervisar/Auditar > Crear informes > Sucesos de GIM
Grupo (Grupo)	Pertenencia a grupos de Guardium. Roles: todos. Portal de usuario: Supervisar/Auditar > Crear informes > Creador de grupos
Actividad de Guardium (AUDITORÍA DE ACTIVIDAD DE USUARIO)	Todas las modificaciones realizadas por los usuarios de Guardium en cualquier entidad de Guardium, como por ejemplo un informe, una definición de consulta o una modificación. Roles: administrador. Portal de usuario: No disponible.

Creador de consultas (dominio)	Descripción
Inicio de sesión de Guardium (INICIO DE SESIÓN DE USUARIO)	Toda la información de inicio y fin de sesión de usuario de Guardium. Roles: administrador. Portal de usuario: No disponible.
Política instalada (Política instalada)	Proporciona una descripción de reglas y parámetros de política para la política instalada. El dominio de Política instalada da soporte a varias políticas y varias acciones por regla. Roles: todos. Portal de usuario: No disponible.
Infracciones de política (INFRACCIONES DE REGLAS DE ACCESO)	Todos los datos de infracciones de política, de todas las infracciones de la política detectadas por los motores de inspección o STAP de Guardium. Roles: todos. Portal de usuario: Supervisar/Auditar > Crear informes > Creador de infracciones de políticas
Resumen de infracciones de política (Infracciones de reglas de acceso)	Todos los datos de infracciones de política, para obtener un resumen de todas las infracciones de la política detectadas por los STAP o los motores de inspección de Guardium. Roles: todos. Portal de usuario: Supervisar/Auditar > Crear informes > Creador de resumen de infracciones de política
Reproducir resultados	Reproduce la corriente de datos desde un origen de datos por otro origen de datos diferente. Roles: ninguno Portal de usuario: no disponible.
Conexiones inesperadas (HUNTER)	Procesos del servidor de bases de datos locales que han evitado que S-TAP se conecte a la base de datos a través de memoria compartida, conductos con nombre u otros medios no estándar. Sólo se aplica a S-TAP en Unix, cuando se utiliza el método de supervisión TEE. Roles: todos. Portal de usuario: Supervisar/Auditar > Crear informes > Creador de conexiones inesperadas
Resultado de asesoramiento de seguridad (Supervisor de resultados de prueba de asesoramiento)	Registra los resultados de los procesos de asesoramiento de vulnerabilidades. Roles: ninguno. Portal de usuario: No disponible.
Uso de almacenamiento intermedio de sniffer (Supervisor de uso de almacenamiento intermedios de sniffer)	Inspección de estadísticas del motor. Roles: ninguno. Portal de usuario: No disponible.
Usuario/Rol/Aplicación (Aplicación Usuario Rol)	Relaciona usuarios, roles y aplicaciones de Guardium (para informar sobre quién tiene acceso a qué aplicaciones de Guardium). Roles: administrador. Portal de usuario: No disponible.
Pruebas de VA (Pruebas de asesoramiento)	Informa sobre pruebas que están disponibles para asesoramientos de seguridad. Roles: administrador Portal de usuario: no disponible.
Cambio de valor (Cambio de valor)	Se realiza un seguimiento de todos los cambios a través de una aplicación que se desencadena en base a cambios de valor. Roles: administrador. Portal de usuario: No disponible.

Tema principal: Dominios, entidades y atributos

Dominios personalizados

Los dominios personalizados permiten dominios definidos por el usuario y pueden definir cualquier tabla de datos que se haya cargado en el dispositivo.

El uso para estos dominios de titularidad personalizados (privilegios) es para los informes de titularidad que se encuentran si se ha iniciado sesión como un usuario. Para ver estos informes, vaya al separador de usuario Titularidades de BD.

Se han predefinido una serie de dominios personalizados.

[Custom] Access

Este dominio contiene todas las mismas entidades que el dominio de Acceso a datos estándar. Se proporciona como un dominio personalizado para permitir que se creen dominios definidos por el usuario adicionales que incluyan información de este dominio y cualquier tabla personalizada que haya sido cargada por el usuario. El dominio [Custom]Access está pensado para ser clonado. Este dominio se actualiza en cada versión; por lo tanto, no es aconsejable crear informes en este dominio. Para obtener una descripción de las entidades incluidas en el dominio de Access, consulte la descripción del dominio de Access en el tema Dominios.

Información de S-TAP (Gestor central)

Informe: Consulte los informes de S-TAP. En el Gestor central, está disponible un informe adicional, Información de S-TAP. Este informe supervisa los S-TAP de todo el entorno. Suba estos datos utilizando el Creador de tablas personalizadas.

La información de S-TAP es un dominio personalizado predefinido que contiene la entidad Información de S-TAP y que no es modificable.

Al definir una consulta personalizada, vaya a la página de subir y pulse en Comprobar/Reparar para crear la tabla personalizada en la base de datos CUSTOM, de lo contrario, guardar consulta no la validará. Esta tabla se carga automáticamente desde todos los orígenes remotos. Un usuario no puede seleccionar los orígenes remotos que se utilizarán, se extraen de todos ellos.

Basándose en esta tabla personalizada y en este dominio personalizado, hay dos informes:

Vista de S-TAP de empresa, desde el Gestor central, información sobre un S-TAP activo en un recopilador y/o unidad gestionada (Si hay duplicados para el mismo motor de S-TAP, uno activo y el otro inactivo, el informe solo utilizará el activo).

La vista de S-TAP de empresa detallada muestra, desde el Gestor central, información de todos los S-TAP activos y pasivos en todos los recopiladores y/o unidades gestionadas.

Si la vista S-TAP de empresa y la vista S-TAP de empresa detallada tienen el mismo aspecto, es porque sólo hay un S-TAP en una unidad gestionada que se está visualizando. La vista S-TAP de empresa detallada tendrá un aspecto distinto si hay más S-TAP y más unidades gestionadas implicadas.

Estos dos informes se pueden elegir desde el separador de supervisión de TAP en un sistema autónomo, pero no visualizarán información.

Dominios de titularidad de BD

Junto con la autenticación de usuarios y la restricción de privilegios de acceso basados en roles a los datos, incluso para los usuarios de bases de datos con más privilegios, existe la necesidad de realizar revisiones de derechos periódicamente, el proceso de validación y garantizar que los usuarios sólo tengan los privilegios necesarios para realizar sus tareas. Esto también se conoce como informe de certificación de derechos de usuario de base de datos.

Utilice los informes de titularidad (privilegio) de base de datos predefinidos de Guardium (por ejemplo) para ver quién tiene privilegios de sistema y quién ha otorgado estos privilegios a otros usuarios y roles. Los informes de titularidad de base de datos son importantes para los auditores que realizan seguimientos de los cambios en el acceso a la base de datos y para garantizar que no existen los agujeros de seguridad de cuentas persistentes o privilegios mal otorgados.

Los Informes de titularidad de BD utilizan la característica Dominio personalizado para crear enlaces entre los datos externos de la base de datos seleccionada con los datos internos de los informes de titularidad predefinidos. Consulte el apartado Informes de titularidades de base de datos para obtener más información sobre cómo utilizar los informes de titularidad de base de datos predefinidos. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador Titularidades de BD.

Nota: Los Informes de titularidades de BD son componentes opcionales habilitados por la clave de producto. Si estos componentes no se han habilitado, las opciones no aparecerán en las selecciones de Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas.

Los informes de titularidad predefinidos se listan a continuación. Aparecen como nombres de dominio en las selecciones de Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas.

- Titularidades de BD de Oracle
- Titularidades de BD de MYSQL
- Titularidades de BD de DB2
- Titularidades de BD de SYBASE
- Titularidades de BD de Informix
- Titularidades de BD de MSSQL 2000
- Titularidades de BD de MSSQL 20005/2008
- Titularidades de BD de Netezza
- Titularidades de BD de Teradata
- Titularidades de BD de PostgreSQL

Titularidades de BD de Oracle

Se proporcionan los siguientes dominios para facilitar la carga y notificación de las Titularidades de BD de Oracle. Cada uno de los siguientes dominios tiene una sola entidad (con el mismo nombre), y hay un informe predefinido para cada dominio. Todos estos dominios están disponibles en las selecciones Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas. Al igual que con otras entidades e informes predefinidos, éstos no se pueden modificar, pero puede clonar y, a continuación, personalizar sus propias versiones de cualquiera de estos informes o dominios. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador Titularidades de BD.

Oracle

- ORA: Cuentas de ALTER SYSTEM - Cuentas con privilegios ALTER SYSTEM y ALTER SESSION
- ORA: Cuentas con BECOME USER - Cuentas con privilegios BECOME USER
- Todas las opc. de priv. y de admin. del sist. de ORA - Informe que muestra todos los privilegios del sistema y la opción admin para usuarios y roles
- Priv. de obj. y columnas de ORA - Privilegios de objetos y columnas otorgados (con o sin opción de otorgar)
- Acceso a objetos ORA mediante PUBLIC - Acceso a objetos mediante PUBLIC
- Privilegios de objetos ORA - Privilegios de objetos mediante la cuenta de base de datos no en el rol SYS y no en el rol DBA
- Ej. priv. de ORA PUBLIC en proc. SYS - Privilegio de ejecución en procedimientos SYS PL/SQL asignados a PUBL
- Roles otorgados de ORA - Roles otorgados a usuarios y roles
- Priv. de sis. de ORA otorgado - Informe jerárquico que muestra el privilegio de sistema otorgado a los usuarios que incluye las definiciones recursivas (es decir, privilegios asignados a los roles y, a continuación, estos roles asignados a los usuarios)
- ORA: Cuentas SYSDBA y SYSOPER - Cuentas con los privilegios SYSDBA y SYSOPER

Para que las titularidades puedan subir datos desde varios orígenes de datos, el requisito general es que el inicio de sesión, que se utiliza para acceder a la base de datos, pueda leer las tablas utilizadas en la consulta (que está oculta para todas las titularidades).

La siguiente lista (con cabecera de línea de comentarios) detalla los privilegios mínimos necesarios, en la tabla de base de datos (o vista de la tabla de base de datos), para que la titularidad funcione.

/* Es necesario seleccionar un privilegio para estas tablas/vistas */

grant select on sys.dba_tab_privs to sqlguard;

grant select on sys.dba_roles to sqlguard;

grant select on sys.dba_users to sqlguard;

grant select on sys.dba_role_privs to sqlguard;

grant select on sys.dba_sys_privs to sqlguard;

grant select on sys.obj$ to sqlguard;

grant select on sys.user$ to sqlguard;

grant select on sys.objauth$ to sqlguard;

grant select on sys.table_privilege_map to sqlguard;

grant select on sys.dba_objects to sqlguard;

grant select on sys.v_$pwfile_users to sqlguard;

grant select on sys.dba_col_privs to sqlguard;

Titularidades de BD de MYSQL

Se proporcionan los siguientes dominios para facilitar la carga y la creación de informes sobre las Titularidades de BD de MYSQL. Cada uno de los siguientes dominios tiene una sola entidad (con el mismo nombre), y hay un informe predefinido para cada dominio. Todos estos dominios están disponibles en las selecciones Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas. Al igual que con otras entidades e informes predefinidos, éstos no se pueden modificar, pero puede clonar y, a continuación, personalizar sus propias versiones de cualquiera de estos informes o dominios. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador Titularidades de BD.

MYSQL: Las consultas que terminan en _40 utilizan la versión más básica del esquema de mysql (para MySQL 4.0 y posterior). information_schema no ha cambiado desde que se introdujo en MySQL 5.0, por lo que hay un conjunto de _50 consultas, pero no hay _51 consultas. Las _50 consultas funcionan para MySQL 5.0 y 5.1 y para 6.0 cuando salga, ya que no se espera que information_schema cambie en 6.0. Las consultas que terminan en _502 (MYSQL502) utilizan el nuevo information_schema, que contiene mucha más información y es mucho más parecido a un diccionario de datos verdadero.

- Privilegios 40 de base de datos de MYSQL
- Privilegios 40 de usuario de MYSQL
- Privilegios 40 de host de MYSQL
- Privilegios 40 de tabla de MYSQL
- Privilegios 500 de base de datos de MYSQL
- Privilegios 500 de usuario de MYSQL
- Privilegios 500 de host de MYSQL
- Privilegios 500 de tabla de MYSQL
- Privilegios 502 de base de datos de MYSQL
- Privilegios 502 de usuario de MYSQL
- Privilegios 502 de host de MYSQL
- Privilegios 502 de tabla de MYSQL

Para que las titularidades puedan subir datos desde varios orígenes de datos, el requisito general es que el inicio de sesión, que se utiliza para acceder a la base de datos, pueda leer las tablas utilizadas en la consulta (que está oculta para todas las titularidades).

La siguiente lista detalla los privilegios mínimos necesarios, en la tabla de base de datos (o vista de la tabla de base de datos), para que la titularidad funcione.

Nota: Además de los privilegios necesarios, el usuario debe conectarse a la base de datos de MYSQL para subir los datos.

Las consultas de titularidad para todas las versiones de MySQL a través de MySQL 5.0.1 utilizan este conjunto de tablas: mysql.db mysql.host mysql.tables_priv mysql.user

A partir de MySQL 5.0.2, y para todas las versiones posteriores, las consultas de titularidad utilizan este conjunto de tablas: information_schema.SCHEMA_PRIVILEGES mysql.host information_schema.TABLE_PRIVILEGES information_schema.USER_PRIVILEGES

Si un origen de datos tiene un tipo de base de datos MYSQL, pero no tiene un nombre de BD (consulte Definiciones de orígenes de datos, el nombre de la base de datos bajo Ubicación está en blanco), los datos de subida entrarán en bucle a través de todas las bases de datos MYSQL a las que tenga acceso el usuario.

Titularidades de BD de DB2

Se proporcionan los dominios siguientes para facilitar la carga y la creación de informes en Titularidades de BD de DB2. Cada uno de los siguientes dominios tiene una sola entidad (con el mismo nombre), y hay un informe predefinido para cada dominio. Todos estos dominios están disponibles en las selecciones Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas. Al igual que con otras entidades e informes predefinidos, éstos no se pueden modificar, pero puede clonar y, a continuación, personalizar sus propias versiones de cualquiera de estos informes o dominios. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador Titularidades de BD.

- Privilegios a nivel de columna de DB2 (SELECT, UPDATE, ETC.)
- Privilegios a nivel de base de datos de DB2 (CONNECT, CREATE, ETC.)
- Privilegios a nivel de índice de DB2 (CONTROL)
- Privilegios a nivel de paquete de DB2 (en paquetes de código – BIND, EXECUTE, ETC.)
- Privilegios a nivel de tabla de DB2 (SELECT, UPDATE, ETC.) Resumen de privilegios de DB2

Para que las titularidades puedan subir datos desde varios orígenes de datos, el requisito general es que el inicio de sesión, que se utiliza para acceder a la base de datos, pueda leer las tablas utilizadas en la consulta (que está oculta para todas las titularidades).

La siguiente lista (con cabecera de línea de comentarios) detalla los privilegios mínimos necesarios, en la tabla de base de datos (o vista de la tabla de base de datos), para que la titularidad funcione.

/* Es necesario seleccionar un privilegio para estas tablas/vistas */

GRANT SELECT ON SYSCAT.COLAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.DBAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.INDEXAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.PACKAGEAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.DBAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.TABAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.SCHEMAAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.PASSTHRUAUTH TO SQLGUARD;

Titularidades de BD de SYBASE

Se proporcionan los siguientes dominios para facilitar la carga y la creación de informes en Titularidades de BD de SYBASE. Cada uno de los siguientes dominios tiene una sola entidad (con el mismo nombre), y hay un informe predefinido para cada dominio. Todos estos dominios están disponibles en las selecciones Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas. Al igual que con otras entidades e informes predefinidos, éstos no se pueden modificar, pero puede clonar y, a continuación, personalizar sus propias versiones de cualquiera de estos informes o dominios. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador Titularidades de BD.

- Privilegio de sistema de SYBASE y roles otorgados al usuario incluyendo la opción de Otorgar
- Rol de SYBASE otorgado a privilegios de usuario y sistema otorgado al usuario y al rol incluyendo la opción de Otorgar
- Acceso de objeto de SYBASE por público
- Privilegio de ejecución de SYBASE en el procedimiento, función asignada a Public
- Cuentas de SYBASE con Roles de administración del sistema o de seguridad
- Privilegio de objetos y columnas de SYBASE otorgado con la opción de Otorgar
- Rol de SYBASE otorgado a usuario

Para que las titularidades puedan subir datos desde varios orígenes de datos, el requisito general es que el inicio de sesión, que se utiliza para acceder a la base de datos, pueda leer las tablas utilizadas en la consulta (que está oculta para todas las titularidades).

La siguiente lista (con cabecera de línea de comentarios) detalla los privilegios mínimos necesarios, en la tabla de base de datos (o vista de la tabla de base de datos), para que la titularidad funcione.

/* Es necesario seleccionar un privilegio para estas tablas/vistas */

/* Son necesarios en la base de datos MASTER */

grant select on master.dbo.sysloginroles to sqlguard

grant select on master.dbo.syslogins to sqlguard

grant select on master.dbo.syssrvroles to sqlguard

/*Son necesarios en cada base de datos, incluida MASTER */

grant select on sysprotects to sqlguard

grant select on sysusers to sqlguard

grant select on sysobjects to sqlguard

grant select on sysroles to sqlguard

Si un origen de datos tiene un tipo de base de datos de SYBASE, pero no tiene un nombre de BD (consulte Definiciones de orígenes de datos, el nombre de la base de datos bajo Ubicación está en blanco), los datos de subida entrarán en bucle a través de todas las bases de datos de SYBASE a las que tenga acceso el usuario.

Titularidades de BD de Informix

Se proporcionan los dominios siguientes para facilitar la carga y la creación de informes en Titularidades de BD de Informix. Cada uno de los siguientes dominios tiene una sola entidad (con el mismo nombre), y hay un informe predefinido para cada dominio. Todos estos dominios están disponibles en las selecciones Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas. Al igual que con otras entidades e informes predefinidos, éstos no se pueden modificar, pero puede clonar y, a continuación, personalizar sus propias versiones de cualquiera de estos informes o dominios. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador Titularidades de BD.

- Privilegios de objetos de Informix mediante la cuenta de base de datos no incluidos la cuenta ni los roles del sistema
- Privilegios, roles y lenguaje a nivel de base de datos de Informix otorgados al usuario, incluida la opción de otorgar
- Privilegios, roles y lenguaje a nivel de base de datos de Informix otorgados al usuario y al rol, incluida la opción de otorgar
- Objeto de Informix otorgado a Public
- Privilegio de ejecución de Informix en el procedimiento y la función de Informix otorgados a Public
- Cuenta de Informix con privilegios de objetos y columnas de Informix de privilegio de DBA otorgados con la opción de Otorgar
- Rol de Informix otorgado a usuario y rol

Para que las titularidades puedan subir datos desde varios orígenes de datos, el requisito general es que el inicio de sesión, que se utiliza para acceder a la base de datos, pueda leer las tablas utilizadas en la consulta (que está oculta para todas las titularidades). La siguiente lista (con cabecera de línea de comentarios) detalla los privilegios mínimos necesarios, en la tabla de base de datos (o vista de la tabla de base de datos), para que la titularidad funcione.

/* Es necesario seleccionar un privilegio para estas tablas/vistas */

Puesto que todos los usuarios tienen privilegios suficientes para los privilegios SELECT del catálogo del sistema, no hay necesidad de otorgar privilegios a ningún usuario. Parece que a Informix no le gusta otorgar el catálogo del sistema a los usuarios. Se utilizaría normalmente la concesión. Pero en este caso, no son necesarios.

grant select on systables to sqlguard;

grant select on systabauth to sqlguard;

grant select on sysusers to sqlguard;

grant select on sysroleauth to sqlguard;

grant select on syslangauth to sqlguard;

grant select on sysroutinelangs to sqlguard;

grant select on sysprocauth to sqlguard;

grant select on sysprocedures to sqlguard;

grant select on syscolauth to sqlguard;

Si un origen de datos tiene un tipo de base de datos de Informix, pero no tiene un nombre de BD (consulte Definiciones de orígenes de datos, el nombre de la base de datos bajo Ubicación está en blanco), los datos de subida entrarán en bucle a través de todas las bases de datos de Informix a las que tenga acceso el usuario.

Titularidades de BD de MSSQL 2000

Se proporcionan los siguientes dominios para facilitar la carga y la creación de informes en Titularidades de BD de MSSQL 2000. Cada uno de los siguientes dominios tiene una sola entidad (con el mismo nombre), y hay un informe predefinido para cada dominio. Todos estos dominios están disponibles en las selecciones Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas. Al igual que con otras entidades e informes predefinidos, éstos no se pueden modificar, pero puede clonar y, a continuación, personalizar sus propias versiones de cualquiera de estos informes o dominios. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador **Titularidades de BD**.

- Privilegios de objetos de MSSQL2000 mediante la cuenta de base de datos no incluido el usuario predeterminado del sistema
- Privilegios de rol/sistema de MSSQL2000 otorgados al Usuario incluida la opción de otorgar
- Roles de MSSQL2000 otorgados a usuario y rol. Privilegios del sistema otorgados a Usuario y Rol incluida la opción de otorgar
- Acceso a objetos de MSSQL2000 por PUBLIC
- Privilegio de ejecución de MSSQL2000 en funciones y procedimientos del sistema a PUBLIC
- Cuentas de base de datos de MSSQL2000 con el rol db_owner y db_securityadmin
- Cuenta de Servidor de MSSQL2000 con sysadmin, serveradmin y security admin /* ejecutar esta titularidad sólo en la base de datos MASTER */
- Privilegios de objetos y columnas de MSSQL2000 otorgados con la opción de otorgar
- Rol de MSSQL2000 otorgado a un usuario y rol

Para que las titularidades puedan subir datos desde varios orígenes de datos, el requisito general es que el inicio de sesión, que se utiliza para acceder a la base de datos, pueda leer las tablas utilizadas en la consulta (que está oculta para todas las titularidades).

La siguiente lista (con cabecera de línea de comentarios) detalla los privilegios mínimos necesarios, en la tabla de base de datos (o vista de la tabla de base de datos), para que la titularidad funcione.

/* Es necesario seleccionar un privilegio para estas tablas/vistas */

/* Son necesarios en la base de datos MASTER */

grant select on dbo.syslogins to sqlguard

/*Son necesarios en cada base de datos, incluida MASTER */

grant select on dbo.sysprotects to sqlguard

grant select on dbo.sysusers to sqlguard

grant select on dbo.sysobjects to sqlguard

grant select on dbo.sysmembers to sqlguard

Si un origen de datos tiene un tipo de base de datos de MSSQL, pero no tiene un nombre de BD (consulte Definiciones de orígenes de datos, el nombre de la base de datos bajo Ubicación está en blanco), los datos de subida entrarán en bucle a través de todas las bases de datos de MSSQL a las que tenga acceso el usuario.

Titularidades de BD de MSSQL 20005/2008

Se proporcionan los siguientes dominios para facilitar la carga y la creación de informes en Titularidades de BD de MSSQL 2005 o MSSQL 2008. Cada uno de los siguientes dominios tiene una sola entidad (con el mismo nombre), y hay un informe predefinido para cada dominio. Todos estos dominios están disponibles en las selecciones Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas. Al igual que con otras entidades e informes predefinidos, éstos no se pueden modificar, pero puede clonar y, a continuación, personalizar sus propias versiones de cualquiera de estos informes o dominios. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador **Titularidades de BD**.

Nota: Los dominios de titularidad para MSSQL2005 listado cubren también MSSQL2008.

- Privilegios de objetos de MSSQL2005/8 mediante la cuenta de base de datos no incluido el usuario predeterminado del sistema.
- Privilegios de rol/sistema de MSSQL2005/8 otorgados a Usuario
- Privilegios de rol/sistema de MSSQL2005/8 otorgados a usuario y rol incluida la opción de otorgar
- Acceso a objetos de MSSQL2005/8 por PUBLIC

- Privilegio de ejecución de MSSQL2005/8 en procedimientos y funciones del sistema en PUBLIC
- Cuentas de base de datos de MSSQL2005/8 del rol db_owner y db_securityadmin
- Cuenta de servidor de MSSQL2005/8 de sysadmin, serveradmin y security admin /* ejecutar sólo en la base de datos MASTER */
- Privilegios de objetos y columnas de MSSQL2005/8 otorgados con la opción de otorgar
- Rol de MSSQL2005/8 otorgado a un usuario y rol.

Para que las titularidades puedan subir datos desde varios orígenes de datos, el requisito general es que el inicio de sesión, que se utiliza para acceder a la base de datos, pueda leer las tablas utilizadas en la consulta (que está oculta para todas las titularidades).

La siguiente lista (con cabecera de línea de comentarios) detalla los privilegios mínimos necesarios, en la tabla de base de datos (o vista de la tabla de base de datos), para que la titularidad funcione.

/* Es necesario seleccionar un privilegio para estas tablas/vistas */

/* Son necesarios en la base de datos MASTER */

grant select on sys.server_principals to sqlguard

/*Son necesarios en cada base de datos incluida MASTER */

grant select on sys.database_permissions to sqlguard

grant select on sys.database_principals to sqlguard

grant select on sys.all_objects to sqlguard

grant select on sys.database_role_members to sqlguard

grant select on sys.columns to sqlguard

Si un origen de datos tiene un tipo de base de datos de MSSQL, pero no tiene un nombre de BD (consulte Definiciones de orígenes de datos, el nombre de la base de datos bajo Ubicación está en blanco), los datos de subida entrarán en bucle a través de todas las bases de datos de MSSQL a las que tenga acceso el usuario.

Titularidades de BD de Netezza

Se proporcionan los siguientes dominios para facilitar la carga y la creación de informes en Titularidades de BD de Netezza. Cada uno de los siguientes dominios tiene una sola entidad (con el mismo nombre), y hay un informe predefinido para cada dominio. Todos estos dominios están disponibles en las selecciones Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas. Al igual que con otras entidades e informes predefinidos, éstos no se pueden modificar, pero puede clonar y, a continuación, personalizar sus propias versiones de cualquiera de estos informes o dominios. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador **Titularidades de BD**.

Nota: No hay ninguna traducción del texto de error de BD para Netezza. El error aparece en la descripción de la excepción. Los usuarios pueden clonar/añadir un informe con la descripción de la excepción para Netezza según sea necesario.

- Netezza: Privs. de obj. por nombre de usuario de BD - Privilegios de objetos con o sin la opción de otorgar mediante el nombre de usuario de la base de datos excluida la cuenta ADMIN.
- Netezza: Privs. de admin. por nombre de usuario de BD - Privilegios de administración con o sin la opción de otorgar mediante el nombre de usuario de la base de datos excluida la cuenta ADMIN.
- Grupo/rol de Netezza otorgado a un usuario - Grupo (Rol) otorgado al usuario
- Privs. de obj. de Netezza por grupo - Privilegios de objetos con o sin la opción de otorgar mediante GROUP excluido PUBLIC.
- Privs. de admin. de Netezza por grupo - Privilegios de administración con o sin la opción de otorgar mediante GROUP excluido PUBLIC.
- Netezza: Privs. de admin. por nombre de usuario de BD, grupo - Privilegios de administración con o sin la opción de otorgar mediante nombre de usuario de base de datos, grupo excluida la cuenta ADMIN y el grupo PUBLIC.
- Privs. de obj. de Netezza otorgados - Privilegios de objeto otorgados con o sin la opción de otorgar a PUBLIC.
- Privs. de admin. de Netezza otorgados - Privilegios de administración otorgados con o sin la opción de otorgar a PUBLIC.
- Priv. de admin. global de Netezza para usuarios y grupos - Privilegios de administración globales otorgados a usuarios y grupos excluida la cuenta ADMIN.
- Priv. de obj. global de Netezza para usuarios y grupos - Privilegios de objetos globales otorgados a usuarios y grupos excluida la cuenta ADMIN.

Para que las titularidades puedan subir datos desde varios orígenes de datos, el requisito general es que el inicio de sesión, que se utiliza para acceder a la base de datos, pueda leer las tablas utilizadas en la consulta (que está oculta para todas las titularidades).

La siguiente lista (con cabecera de línea de comentarios) detalla los privilegios mínimos necesarios, en la tabla de base de datos (o vista de la tabla de base de datos), para que la titularidad funcione.

/* Es necesario seleccionar un privilegio para estas tablas/vistas */

/* Este script se debe ejecutar desde la base de datos del sistema */

GRANT SELECT ON SYSTEM VIEW TO sqlguard;

GRANT LIST ON DATABASE TO sqlguard;

GRANT LIST ON USER TO sqlguard;

GRANT LIST ON GROUP TO sqlguard;

GRANT SELECT ON _V_CONNECTION TO sqlguard;

Para las consultas de titularidad de Netezza, se recomienda conectarse a la base de datos SYSTEM, especialmente cuando se otorga el privilegio al usuario que va a ejecutar estos informes. La otorgación del privilegio DEBE tener lugar desde la base de datos SYSTEM o, de lo contrario, el privilegio otorgado sólo tendrá lugar en una base de datos determinada. Cuando el privilegio otorgado tiene lugar desde la base de datos SYSTEM, una característica especial permitirá que el privilegio otorgado se lleve a cabo en todas las bases de datos.

Titularidades de BD de Teradata

Se proporcionan los siguientes dominios para facilitar la carga y la creación de informes en Titularidades de BD de Teradata. Cada uno de los siguientes dominios tiene una sola entidad (con el mismo nombre), y hay un informe predefinido para cada dominio. Todos estos dominios están disponibles en las selecciones Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas. Al igual que con otras entidades e informes predefinidos, éstos no se pueden modificar, pero puede clonar y, a continuación, personalizar sus propias versiones de cualquiera de estos informes o dominios. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador **Titularidades de BD**.

- Privilegios de objetos de Teradata mediante la cuenta de base de datos no incluidos los usuarios predeterminados del sistema.
- Privilegios y roles del sistema de Teradata otorgados a usuarios incluida la opción de otorgar.
- Roles de Teradata otorgados a usuarios y roles incluida la opción de otorgar.
- Roles de Teradata otorgados a usuarios y roles. Privilegios del sistema otorgados a usuarios y roles incluida la opción de otorgar.
- Privilegios de objetos y sistema de Teradata otorgados a público. Tenga en cuenta que el rol no se puede otorgar a público en Teradata.
- Privilegios de ejecución de Teradata en objetos de base de datos del sistema a público.
- Administración del sistema de Teradata, privilegios de administración de seguridad otorgados a usuario y rol.
  Nota: No hay tal rol de Administrador de seguridad ni de sistema en Teradata. El usuario debe crear sus propios roles. Estos son algunos privilegios de sistema importantes que normalmente no se otorgarían a un usuario normal: ABORT SESSION, CREATE DATABASE, CREATE PROFILE, CREATE ROLE,CREATE USER, DROP DATABASE, DROP PROFILE, DROP ROLE, DROP USER, MONITOR RESOURCE, MONITOR SESSION, REPLICATION OVERRIDE, SET SESSION RATE, SET RESOURCE RATE.
- Privilegios de objetos de Teradata otorgados con la opción granted a usuarios. No se incluye DBC ni receptor de autorización = 'All'.

Para que las titularidades puedan subir datos desde varios orígenes de datos, el requisito general es que el inicio de sesión, que se utiliza para acceder a la base de datos, pueda leer las tablas utilizadas en la consulta (que está oculta para todas las titularidades).

La siguiente lista (con cabecera de línea de comentarios) detalla los privilegios mínimos necesarios, en la tabla de base de datos (o vista de la tabla de base de datos), para que la titularidad funcione.

/* Es necesario seleccionar un privilegio para estas tablas/vistas */

GRANT SELECT ON DBC.AllRights TO sqlguard;

GRANT SELECT ON DBC.Tables TO sqlguard;

GRANT SELECT ON DBC.AllRoleRights TO sqlguard;

GRANT SELECT ON DBC.RoleMembers TO sqlguard;

Titularidades de BD de PostgreSQL

Se proporcionan los siguientes dominios para facilitar la carga y la creación de informes en Titularidades de BD de PostgreSQL. Cada uno de los siguientes dominios tiene una sola entidad (con el mismo nombre), y hay un informe predefinido para cada dominio. Todos estos dominios están disponibles en las selecciones Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas. Al igual que con otras entidades e informes predefinidos, éstos no se pueden modificar, pero puede clonar y, a continuación, personalizar sus propias versiones de cualquiera de estos informes o dominios. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador **Titularidades de BD**.

Hay siete dominios/consultas/informes personalizados de titularidad para PostgreSQL. Son los siguientes (cada uno de ellos se lista con el nombre, la descripción y la nota de Informe):

- Priv. de PostgreSQL en bases de datos otorgadas al rol de usuario público con o sin opción otorgada. Privilegio sobre bases de datos otorgadas a público, usuario y rol con o sin opción otorgada. Ejecútelo en cualquier base de datos, idealmente en PostgreSQL.
- Priv. de PostgreSQL en idioma otorgado al rol de usuario público con o sin opción otorgada. Privilegio sobre el idioma otorgado a público, usuario y rol con o sin la opción otorgada. Ejecútelo por base de datos.
- Priv. de PostgreSQL en esquema otorgado al rol de usuario público con o sin opción otorgada. Privilegio en Esquema otorgado a público, usuario y rol con o sin la opción otorgada. Ejecútelo por base de datos.
- Priv. de PostgreSQL en espacio de tabla otorgado al rol de usuario público con o sin opción otorgada. Privilegio en Espacio de tabla otorgado a público, usuario y rol con o sin la opción otorgada. Ejecútelo en cualquier base de datos, idealmente en PostgreSQL.
- Rol o usuario de PostgreSQL otorgado al usuario o al rol. Rol o usuario otorgado a usuario o rol incluida la opción de otorgar. Ejecútelo una vez en cualquier base de datos. Idealmente PostgreSQL.

- Superusuario de PostgreSQL otorgado a un usuario o rol. Superusuario otorgado a usuario o rol. Ejecútelo una vez en cualquier base de datos. Idealmente PostgreSQL.
- Privs. de sis. de PostgreSQL otorgados a un usuario y a un rol. Privilegios del sistema otorgados a usuario y rol. Ejecútelo una vez en cualquier base de datos. Idealmente PostgreSQL.
- Secuencia de vista de tabla de PostgreSQL y privs. de función otorgados a público. Privilegios de tablas, vistas, secuencia y funciones otorgados a público. Ejecútelo por base de datos. Ejecútelo por base de datos.
- Secuencia de vista de tabla de PostgreSQL y privs. de función otorgados con la opción de otorgar. Privilegios de tablas, vistas, secuencia y privilegios de funciones otorgados al usuario y al rol sólo con la opción de otorgar. Excluir cuenta de PostgreSQL.
- Secuencia de vista de tabla de PostgreSQL y privs. de función otorgados a roles. Privilegios de tablas, vistas, secuencias y funciones otorgados a roles. No se incluye el público. Ejecútelo por base de datos.
- Secuencia de vistas de tabla de PostgreSQL y privs. de funciones otorgados al inicio de sesión. Privilegios de tablas, vistas, secuencia y funciones otorgados a los inicios de sesión. No se incluye el usuario del sistema postgres. Ejecútelo por base de datos.

Nota: A partir de la versión 8.3.6, PostgreSQL no da soporte a la opción grant admin en público. Sólo hay función, sin procedimiento de almacenamiento. No hay soporte para el otorgamiento de columnas, sólo otorgamiento de tabla. Público es un grupo, no un usuario. Público no se muestra en pg_roles. Los únicos privilegios necesarios para ejecutar todas estas consultas es: GRANT CONNECT ON DATABASE PostgreSQL TO username;

Para que las titularidades puedan subir datos desde varios orígenes de datos, el requisito general es que el inicio de sesión, que se utiliza para acceder a la base de datos, pueda leer las tablas utilizadas en la consulta (que está oculta para todas las titularidades).

La siguiente lista (con cabecera de línea de comentarios) detalla los privilegios mínimos necesarios, en la tabla de base de datos (o vista de la tabla de base de datos), para que la titularidad funcione.

/* Es necesario seleccionar un privilegio para estas tablas/vistas */

/*Esto es necesario en la base de datos POSTGRES*/

grant connect on database postgres to sqlguard;

/*Son necesarios en cada base de datos, incluido POSTGRES (De forma predeterminada, ya se han otorgado a PUBLIC) */

grant select on pg_class to sqlguard;

grant select on pg_namespace to sqlguard;

grant select on pg_roles to sqlguard;

grant select on pg_proc to sqlguard;

grant select on pg_auth_members to sqlguard;

grant select on pg_language to sqlguard;

grant select on pg_tablespace to sqlguard;

grant select on pg_database to sqlguard;

Si un origen de datos tiene un tipo de base de datos PostgreSQL, pero no tiene un nombre de BD (consulte Definiciones de orígenes de datos, el nombre de la base de datos bajo Ubicación está en blanco), los datos de subida entrarán en bucle a través de todas las bases de datos de PostgreSQL a las que tenga acceso el usuario.

Tema principal: Dominios, entidades y atributos

Entidades y atributos

Este tema contiene una descripción de los atributos contenidos en cada entidad.

Para obtener una visión general de dominios, entidades y atributos, consulte Dominios, entidades y atributos. Para obtener una descripción de todos los dominios, consulte Dominios.

Para los orígenes de datos de z/OS (Db2, Conjuntos de datos e IMS), hay atributos específicos del origen de datos. Tenga en cuenta que el significado de estos atributos existentes puede ser diferente de lo que se describe aquí. Para obtener más información sobre entidades y atributos específicos de los orígenes de datos de z/OS, consulte lo siguiente:

- Entidades y atributos de informe para conjuntos de datos
- Atributos y entidades de informe para DB2 for z/OS
- Atributos y entidades de informe para IMS

Entidad Política de acceso

Describe todas las políticas disponibles en el sistema. Parecido a la entidad de Políticas instaladas que se utiliza para todas las políticas instaladas en el sistema.

Lista de entidades para Política de acceso - Entidad Política de acceso, Entidad Política de regla; entidad de acción de regla y Notificación de alerta. Consulte la entidad Regla para obtener una lista de atributos. Consulte la entidad Acción de regla para obtener una lista de atributos. Consulte la entidad Notificación de alerta para obtener

una lista de atributos.

Tabla 1. Entidad Periodo de acceso

Atributo	Descripción
ID de política	Identifica de forma exclusiva una política de acceso
Descripción de política	Describe la política de acceso
Seguimiento de auditoría selectivo	Indica si se trata de una política de seguimiento de auditoría selectiva (verdadero/falso).
Patrón de auditoría	Patrón de prueba utilizado para una política de seguimiento de auditoría selectiva.
Indicación de fecha y hora	Indicación de fecha y hora de la creación del registro.

Entidad Periodo de acceso

Los períodos de acceso están relacionados con las sesiones. De forma predeterminada, un periodo de acceso es un intervalo de una hora, sin embargo, esto lo puede cambiar el administrador de Guardium en la configuración del motor de inspección (se corresponde con la granularidad de registro).

Los valores de tiempo de espera dependen del número de las sesiones abiertas por la hebra del analizador. Para cada hebra de analizador hay los siguientes valores predeterminados: Si el número de sesiones abiertas es > 0 y < 250, entonces el tiempo de espera es de 60 minutos. Si el número de sesiones abiertas es >=250 y < 500, el tiempo de espera es de 30 minutos. Si el número de sesiones abiertas es > = 500 y < 750, el tiempo de espera es 15 minutos, si el número de sesiones abiertas es > = 750 y < 1200, entonces el tiempo de espera es de 5 minutos. Si el número de sesiones abiertas es > = 1200, el tiempo de espera es de 2 minutos.

Tabla 2. Entidad Periodo de acceso

Atributo	Descripción
ID de sesión	Identifica una sesión de forma exclusiva.
ID de instancia	Identifica de forma exclusiva una instancia de una construcción.
ID de construcción	Identifica de forma exclusiva una construcción de mandato (por ejemplo, select a from b).
Total accesos	Recuento total de instancias de construcción para este periodo de acceso.
Fecha inicial de periodo	Fecha inicial desde el atributo inicio de periodo.
Día de semana de inicio de periodo	Solo día de la semana desde el atributo inicio del periodo.
Hora de inicio de periodo	Solo fecha desde el atributo periodo de inicio.
Indicación de fecha y hora	Inicialmente, el valor de Indicación de fecha y hora se establece la primera vez que se observa una solicitud en una conexión de cliente-servidor durante un periodo de acceso. De forma predeterminada, un periodo de acceso es un intervalo de una hora, sin embargo, esto lo puede cambiar el administrador de Guardium en la configuración del motor de inspección - -consulte la Guía del administrador de Guardium. A partir de entonces, para cada solicitud posterior, se actualiza cuando el sistema actualiza el tiempo medio de ejecución y el recuento de mandatos para este periodo.
Final de periodo	Fecha y hora para el final del periodo de acceso.
Fecha final del periodo	Solo fecha desde el atributo de final de periodo.
Día de semana de final de periodo	Solo día de la semana desde el atributo de final de periodo.
Hora de final de periodo	Solo hora del atributo de final del periodo.
Usuario de aplicación	Nombre del usuario de la aplicación.
Promedio de tiempo de ejecución	El tiempo medio de ejecución del mandato durante el periodo. Esto sólo es para sentencias SQL. No se aplica al tráfico compartido de archivos Windows o FTP.
SQL con fallos (2)	El número de solicitudes SQL con fallos. Consulte la nota al final de la tabla.
SQL satisfactorios (2)	El número de solicitudes SQL satisfactorias. Consulte la nota al final de la tabla.
ID de suceso de aplicación	ID de suceso de aplicación si se establece desde la API.
Total de registros afectados (2)	Número total de registros afectados. Consulte la nota al final de la tabla.
Promedio registros afectados (2)	Número medio de registros afectados. Consulte la nota al final de la tabla.

Atributo	Descripción
Total de registros afectados (Desc) (2)	Si el atributo Total de registros afectados es una serie de caracteres en lugar de un número, dicho valor aparece aquí (por ejemplo, Conjunto de resultados grande o N/D). Registros afectados - Conjunto de resultados del número de registros que se ven afectados por cada ejecución de sentencias SQL. Nota: La opción de registros afectados es una operación de sniffer que precisa que el sniffer procese paquetes de respuesta adicionales y postponga la creación del registro de datos afectados lo que incrementa el tamaño del almacenamiento intermedio y que potencialmente puede tener un efecto adverso en el rendimiento global del sniffer. El impacto significativo proviene de las respuestas realmente grandes. Para evitar una gran cantidad de sobrecarga asociada por esta operación, Guardium utiliza un conjunto de umbrales predeterminados que permite que el sniffer decida omitir el proceso cuando se superen dichos umbrales. Utilice los mandatos de CLI store max_results_set_size, store max_result_set_packet_size y store max_tds_response_packets para establecer los niveles de granularidad. Ejemplo de valores del conjunto de resultados: • Caso 1, valor de registro afectado, número positivo - esto representa el tamaño correcto del conjunto de resultados. • Caso 2, valor de registro afectado, -2 - Esto significa que el número de registros ha superado el límite configurable (Se puede ajustar desde la interfaz de línea de mandatos). • Caso 3, valor de registro afectado, -1 - Muestra los casos no soportados por Guardium de configuraciones de paquete. • Caso 4, valor de registro afectado, -2 - Si el conjunto de resultados es enviado por la modalidad de corriente. • Caso 5, valor de registro afectado, -2 - Resultado intermedio durante recuento de registro para actualizar al usuario sobre el valor actuar, finaliza con un número positivo del total de registros.
Mostrar segundos	Si se está realizando un seguimiento del número de accesos por segundo, contiene recuentos para cada segundo en el periodo de acceso (normalmente una hora).
Promedio de tiempo de reconocimiento de ejecución	Promedio de tiempo de reconocimiento de ejecución en milisegundos
Huso horario original	Desplazamiento de UTC. Esto es para indicar que se debe establecer un desplazamiento de UTC de forma que el tiempo de dos recopiladores distintos que están en dos husos horarios diferentes agreguen correctamente sus datos. Si no se estableciese el desplazamiento, existiría una condición en la que los usuarios en realidad no serían capaces de determinar o ver una representación verdadera de cuándo ocurrieron las cosas con relación al tiempo. Por ejemplo, en un agregador que agrega datos de husos horarios diferentes, puede ver el inicio de sesión de un registro a las 21:00 con un huso horario original UTC-02:00 y otro registro de inicio de sesión a las 21:00 en un huso horario original UTC-05:00. Esto significa que estos sucesos se produjeron con una diferencia de 3 horas, pero respectivamente en la misma hora (21:00 h).

ID de sesión, ID de instancia, ID de construcción y Total accesos solo están disponibles a los usuarios con el rol de administrador.

SQL con fallos, SQL satisfactorios, ID de suceso de aplicación, Total de registros afectados, Promedio registros afectados y Total de registros afectados (Desc) son atributos que sólo aparecen cuando la entidad principal de la consulta permite este nivel de detalle. Estos no están disponibles si la entidad principal es Cliente/Servidor o Sesión.

Entidad Regla de acceso

Nombre que se asigna a una regla de acceso al definirla. Sólo está disponible para la creación de informes desde la entidad Infracciones de reglas de política (descrita más adelante), cuando se registra una infracción de regla de acceso.

Tabla 3. Entidad Regla de acceso

Atributo	Descripción
Descripción de regla de acceso	Descripción desde la definición de regla de política de acceso.

Entidad Tipos de actividad

Únicamente disponible desde el dominio de Agregación/Archivado, que de forma predeterminada está disponible únicamente para usuarios con el rol de administrador. Sólo se puede acceder a la entidad Tipos de actividad desde la entidad de Registro de agregación/importación/exportación. Identifica un tipo de acción (preparar para agregación, cifrado, envío, etc.).

Tabla 4. Entidad Tipos de actividad

Atributo	Descripción
Tipo de actividad	Descripción de una actividad de agregación/importación/exportación.

Entidad Registro de agregación/archivado

Únicamente disponible desde el dominio de Agregación/Archivado, que de forma predeterminada está disponible únicamente para usuarios con el rol de administrador. Se crean una o más entidades de registro de agregación/importación/exportación para cada actividad. Por ejemplo, cuando un sistema de agregador importa datos, normalmente verá como mínimo cuatro actividades:

Preparar para agregación

Comprobar importación duplicada (una por fila exportada para este agregador)

Extraer (una por fila a fusionar)

Fusionar (una por fila fusionada)

Tabla 5. Entidad Registro de agregación/archivado

Atributo	Descripción
Indicación de fecha y hora	Actualizada al principio y al final de la actividad que se está registrando (preparación para archivado, cifrado, envío, etc.).
Estado	Estado de la actividad de registro de agregación/importación/exportación.
Nombre de usuario	Nombre de usuario bajo el que se inició la actividad.
Hora de inicio	Hora de inicio de la actividad.
Hora de finalización	Hora de finalización de la actividad.
Inicio de periodo	Hora de inicio para los datos sobre los que se está actuando. Cada actividad de archivado o agregación funciona en un día de actividad completo.
Final de periodo	Hora de finalización de la actividad sobre la que se actúa.
Nombre de archivo	Nombre de archivo utilizado para la actividad. Los archivos creados por las operaciones de archivado y exportación se denominan de la siguiente manera: <secuencia_día>-<host_scp>-w<indicación_fecha_hora_ejec>-d<fecha_datos>.dbdump.enc Por ejemplo: 732423-g1.guardium.com-w20050425.040042-d2005-04-22.dbdump.enc La fecha de los datos contenidos en el archivo, en el formato aaaa-mm-dd es fecha_datos, cerca del final del nombre de archivo (justo antes de .dbdump.enc). Tenga cuidado de no confundir esta fecha con la fecha de ejecución, que aparece antes en el nombre de archivo, y que es la fecha en que los datos se han exportado o exportado.
Comentario	Comentario adicional para la actividad.
Nombre de host de Guardium	Nombre del host de Guardium.
Registros depurados	Si el tipo de actividad es Depurar, el número de registros depurados. De lo contrario, N/D.
Huso horario original	Desplazamiento de UTC. Esto se realiza en concreto para los agregadores que tienen recopiladores en distintos husos horarios y, por lo tanto, actividades que se han realizado en distintas horas no parecen como si se hubiesen producido a la misma hora al importarlas al agregador. Por ejemplo, en un agregador que agrega datos de husos horarios diferentes, puede ver el inicio de sesión de un registro a las 21:00 con un huso horario original UTC-02:00 y otro registro de inicio de sesión a las 21:00 en un huso horario original UTC-05:00. Esto significa que estos sucesos se produjeron con una diferencia de 3 horas, pero respectivamente en la misma hora (21:00 h).

Entidad Notificación de alerta

Describe una notificación de alerta de política.

Tabla 6. Entidad Notificación de alerta

Atributo	Descripción
ALERT_NOTIFICATION_ID	Identifica la notificación de alerta.
ALERT_ID	Identifica la definición de alerta.
Tipo de notificación de alerta	Tipo de alerta desde la definición de regla de política.
Usuario de alerta	Receptor de la alerta.
Destino de alerta	Tipo de alerta (EMAIL, SNMP, SYSLOG, CUSTM).
Indicación de fecha y hora	Registro de alerta de indicación de fecha y hora creado.

ALERT_NOTIFICATION_ID y ALERT_ID solo está disponible a usuarios con el rol de administrador.

Entidad Datos de aplicación

Se utiliza para los informes de SAP y Siebel.

Tabla 7. Entidad Datos de aplicación

Atributo	Descripción
ID de datos de aplicación	Identificador exclusivo para estos datos.
Código de aplicación	Código de tipo de aplicación.
ID SQL completo	Identifica los datos de SQL completos.
Tipo de aplicación	Tipo de aplicación.
Usuario	Nombre del usuario de la aplicación.
Tipo de operación	Tipo de la operación.
Fecha de cambio	Fecha del cambio.
Indicación de fecha y hora	Indicación de fecha y hora de este registro.
Nombre de elemento	Nombre del elemento afectado.
Código de transacción	Código de transacción.
ID de sistema	Identificador exclusivo para el sistema.

Atributo	Descripción
Detalle de registro 1	Varía por tipo de elemento.
Detalle de registro 2	Varía por tipo de elemento.
Detalle de registro 3	Varía por tipo de elemento.
Detalle de registro 4	Varía por tipo de elemento.
VBKey	Valor de VBKey.
Huso horario original	Desplazamiento de UTC. Esto se realiza en concreto para los agregadores que tienen recopiladores en distintos husos horarios y, por lo tanto, actividades que se han realizado en distintas horas no parecen como si se hubiesen producido a la misma hora al importarlas al agregador. Por ejemplo, en un agregador que agrega datos de husos horarios diferentes, puede ver el inicio de sesión de un registro a las 21:00 con un huso horario original UTC-02:00 y otro registro de inicio de sesión a las 21:00 en un huso horario original UTC-05:00. Esto significa que estos sucesos se produjeron con una diferencia de 3 horas, pero respectivamente en la misma hora (21:00 h).

Entidad Sucesos de aplicación

Esta entidad se crea cada vez que el sistema observa una llamada de API de sucesos de aplicación (que establece estos valores de atributo) o una llamada de procedimiento almacenado que se ha identificado como un procedimiento de identificación personalizado (que correlaciona parámetros de procedimiento almacenado con estos atributos).

Tabla 8. Entidad Sucesos de aplicación

Atributo	Descripción
ID de suceso de aplicación	Identificador exclusivo para esta entidad de sucesos de aplicación.
Nombre de usuario de suceso	Nombre de usuario, establecido por GuardAppEvent:Start.
Tipo de suceso	Tipo se suceso, establecido por GuardAppEvent:Start.
Serie de valor de suceso	Valor de serie, establecido por GuardAppEvent:Start.
Número de valor de suceso	Valor numérico, establecido por GuardAppEvent:Start.
Fecha de suceso	Valor de fecha/hora, establecido por GuardAppEvent:Start. Se visualiza en el formato aaaa-mm-dd hh:mm:ss. Nota: Si se realiza un intento de establecer la fecha del suceso con un formato distinto de aaaa-mm-dd, contendrá todo ceros. La parte de hora (hh:mm:ss) es opcional, y si se omite será 00:00:00.
Indicación de fecha y hora	Creado sólo una vez, cuando se registra el suceso. No confunda este atributo con el atributo Fecha de suceso, que se puede establecer utilizando una llamada a la API o desde un parámetro de procedimiento almacenado. (Consulte la Guía del administrador de Guardium para obtener una descripción de la API de sucesos de aplicación y los procedimientos de identificación personalizados).
Tipo de liberación de suceso	Tipo de suceso, establecido por GuardAppEvent:Released.
Nombre de usuario de liberación de suceso	Nombre de usuario, establecido por GuardAppEvent: Released.
Serie de valor de liberación de suceso	Valor de serie, establecido por GuardAppEvent: Released.
Número de valor de liberación de suceso	Valor numérico, establecido por GuardAppEvent: Released.
Fecha de liberación de suceso	Valor de fecha/hora, establecido por GuardAppEvent:Released. Se visualiza en el formato aaaa-mm-dd hh:mm:ss.
Huso horario original	Desplazamiento de UTC. Esto se realiza en concreto para los agregadores que tienen recopiladores en distintos husos horarios y, por lo tanto, actividades que se han realizado en distintas horas no parecen como si se hubiesen producido a la misma hora al importarlas al agregador. Por ejemplo, en un agregador que agrega datos de husos horarios diferentes, puede ver el inicio de sesión de un registro a las 21:00 con un huso horario original UTC-02:00 y otro registro de inicio de sesión a las 21:00 en un huso horario original UTC-05:00. Esto significa que estos sucesos se produjeron con una diferencia de 3 horas, pero respectivamente en la misma hora (21:00 h).

El ID de suceso de aplicación sólo está disponible para los usuarios con el rol de administración.

Entidad Nombre de usuario de aplicación

Esta entidad mostrará el nombre de usuario del suceso de aplicación si existe en el mismo. De lo contrario, el nombre de usuario se visualizará desde la instancia de construcción.

Tabla 9. Entidad Nombre de usuario de aplicación

Atributo	Descripción
Nombre de usuario de aplicación	Identificador exclusivo para esta entidad de nombre de usuario de aplicación.

Entidad Registro de asesoramiento

Esta entidad se crea cada vez que se ejecuta un asesoramiento.

Tabla 10. Entidad Registro de asesoramiento

Atributo	Descripción

Atributo	Descripción
ID de registro de asesoramiento	Identifica el asesoramiento de forma exclusiva.
Indicación de fecha y hora	Indicación de fecha y hora del asesoramiento.
Fecha de indicación de fecha y hora	Parte de la fecha de la indicación de fecha y hora.
Hora de indicación de fecha y hora	Parte de la hora de la indicación de fecha y hora.
Tipo de registro de asesoramiento	Predefinido, consulta o prueba personalizada.
Gravedad de registro de asesoramiento	Gravedad de la prueba de asesoramiento: Crítico, Mayor, Menor, Precaución, Informativo. Esta es una lista ordenada del nivel de clasificaciones de gravedad. Gravedad de la prueba de asesoramiento: Crítico, Mayor, Menor, Precaución, Informativo. La gravedad más alta es la primera clasificación de esta lista. La gravedad más baja es la última clasificación de esta lista.
ID1 de resultado de asesoramiento	Identifica el conjunto de resultados del asesoramiento.
Mensaje	Mensaje devuelto por el asesoramiento.
Detalles	Detalles de este asesoramiento.

El ID de registro de asesoramiento solo está disponible a los usuarios con el rol de administrador.

Entidad Origen de datos de resultado de asesoramiento

Esta entidad identifica un origen de datos al que la prueba de asesoramiento accede.

Tabla 11. Entidad Origen de datos de resultado de asesoramiento

Atributo	Descripción
ID de origen de datos de resultado de asesoramiento	Identifica un conjunto de resultados para un origen de datos.
ID de resultado de asesoramiento	Identifica el resultado.
Tipo de BD	Tipo de base de datos: Oracle, MS-SQL, DB2, Sybase, Informix, etc.
Nombre de BD	Nombre de base de datos.
Nivel de versión	Nivel de versión de la base de datos.
Nivel de parche	Nivel de parche de la base de datos.
Información versión completa	Información de versión completa para el origen de datos
Nombre de origen de datos	Nombre del origen de datos.
Descripción	Descripción del origen de datos.
Host	Nombre de host para el origen de datos.
Puerto	Número de puerto en el host.
Nombre de servicio	Nombre de servicio para el origen de datos.
Nombre de usuario	Nombre de usuario utilizado para el acceso al origen de datos.

ID de origen de datos de resultado de asesoramiento y el ID de resultado de asesoramiento sólo están disponibles para los usuarios con el rol de administrador.

Entidad Cabecera de resultado de asesoramiento

Esta entidad se crea para cada tarea del conjunto de resultados del asesoramiento.

Tabla 12. Entidad Cabecera de resultado de asesoramiento

Atributo	Descripción
ID de resultado de asesoramiento	Identifica el conjunto de resultados del asesoramiento.
ID de asesoramiento	Identificación del asesoramiento.
ID de tarea	Identifica la tarea dentro del asesoramiento.
Distintivo de parámetro modificado	Indica si los parámetros se han modificado desde la última ejecución.
Fecha de ejecución	Fecha en la que se ejecutó el asesoramiento.
Recibido por todos	Indica si estos resultados han sido recibidos por todos los receptores en la lista de distribución.
Puntuación global	Puntuación global para el asesoramiento.
Desde fecha	Desde fecha para el asesoramiento.
Hasta fecha	Hasta fecha para el asesoramiento.
Descripción de asesoramiento	Nombre de asesoramiento desde la definición.

Atributo	Descripción
Filtrar IP de cliente	Clientes seleccionados: dirección IP exacta, dirección con comodines (*) o vacía para seleccionar todo.
Filtrar IP de servidor	Servidores seleccionados: dirección IP exacta, dirección con comodines (*) o vacía para seleccionar todo.
Recomendación	Recomendación devuelta para la tarea.

ID de resultado de asesoramiento, ID de asesoramiento e ID de tarea solo están disponibles a los usuarios con el rol de administrador.

Entidad Pruebas de asesoramiento

Esta entidad contiene entradas para las pruebas disponibles.

Tabla 13. Entidad Pruebas de asesoramiento

Atributo	Descripción
Descripción de la prueba	Descripción de texto de la prueba
Tipo de prueba	Tipo de prueba de asesoramiento (Observado, Predefinido, Personalizado, Basado en consultas, CVE)
Tipo de origen de datos	Tipo de origen de datos (DB2, Informix, MYSQL, ORACLE, SYBASE, etc.)
Umbral	Umbral definido por el usuario, para modificar el valor definido al crear de la prueba
Valor predeterminado de umbral	Umbral predeterminado que define los criterios de éxito/fallo
Gravedad	Gravedad del asesoramiento (Crítico, Mayor, Menor, Precaución, Información)
Categoría	Categoría del asesoramiento (Privilegio, Autenticación, Configuración, Versión, Otros)
Indicación de fecha y hora	Indicación de fecha y hora en la que se creó la prueba

Entidad Proceso de auditoría

Esta entidad contiene parámetros de definición básicos para un proceso de auditoría.

Tabla 14. Entidad Proceso de auditoría

Atributo	Descripción
Descripción de proceso	Descripción de la definición del proceso de auditoría.
Activo	Indica si el proceso está activo (capaz de ser planificado).
Mantener resultados - Días	Número de días que el sistema conservará los resultados.
Mantener resultados - Cantidad	Número de días que el sistema conservará los conjuntos de resultados.

Entidad Comentarios de proceso de auditoría

Esta entidad tiene comentarios adjuntados a una definición de proceso de auditoría. Los comentarios adjuntados a los resultados del proceso de auditoría están contenidos en la entidad Comentarios de proceso de auditoría.

Tabla 15. Entidad Comentarios de proceso de auditoría

Atributo	Descripción
Comentario de proceso de auditoría	Texto del comentario.
Creador de comentario de proceso de auditoría	Creador del comentario.
Indicación de fecha y hora del comentario de proceso de auditoría	Indicación de fecha y hora para el comentario.

Entidad Tarea de auditoría

Esta entidad describe una tarea de auditoría individual (dentro de un proceso de auditoría).

Tabla 16. Entidad Tarea de auditoría

Atributo	Descripción
Tipo de tarea	Un valor numérico indica si la tarea es un informe, un asesoramiento de seguridad, un seguimiento de auditoría de entidad, un conjunto de privacidad o un proceso de clasificación. Los alias se definen para estos tipos, por lo que los informes con alias simplificarán la lectura de la salida del informe.
Descripción de tarea	Nombre de la tarea desde la definición de tarea.

Entidad Resultado del proceso de auditoría

Esta entidad contiene la fecha de ejecución de un conjunto de resultados del proceso de auditoría.

Tabla 17. Entidad Resultado del proceso de auditoría

Atributo	Descripción
Fecha de ejecución	Fecha en la que se ejecutó el proceso de auditoría.

Entidad Comentarios de resultados de proceso de auditoría

Esta entidad tiene comentarios adjuntados a unos resultados del proceso de auditoría. Los comentarios adjuntados a una definición de proceso de auditoría están contenidos en la entidad Comentarios de proceso de auditoría.

Tabla 18. Entidad Comentarios de resultados de proceso de auditoría

Atributo	Descripción
Comentario de proceso de auditoría	Texto del comentario.
Creador de comentario de proceso de auditoría	Creador del comentario.
Indicación de fecha y hora del comentario de proceso de auditoría	Indicación de fecha y hora del comentario

Entidad Escaneo de descubrimiento automático

Esta entidad identifica cuándo se ha ejecutado un escaneo.

Tabla 19. Entidad Escaneo de descubrimiento automático

Atributo	Descripción
Indicación de fecha y hora de escaneo	Hora de ejecución del escaneo.
Huso horario original	Desplazamiento de UTC. Esto se realiza en concreto para los agregadores que tienen recopiladores en distintos husos horarios y, por lo tanto, actividades que se han realizado en distintas horas no parecen como si se hubiesen producido a la misma hora al importarlas al agregador. Por ejemplo, en un agregador que agrega datos de husos horarios diferentes, puede ver el inicio de sesión de un registro a las 21:00 con un huso horario original UTC-02:00 y otro registro de inicio de sesión a las 21:00 en un huso horario original UTC-05:00. Esto significa que estos sucesos se produjeron con una diferencia de 3 horas, pero respectivamente en la misma hora (21:00 h).

Entidad Columnas cambiadas

Esta entidad describe una columna cambiada.

Tabla 20. Entidad Columnas cambiadas

Atributo	Descripción
Nombre de columna cambiado	Nombre de columna cambiado en la base de datos.
Valor antiguo	Valor anterior al cambio.
Valor nuevo	Valor después del cambio.
Huso horario original	Desplazamiento de UTC. Esto se realiza en concreto para los agregadores que tienen recopiladores en distintos husos horarios y, por lo tanto, actividades que se han realizado en distintas horas no parecen como si se hubiesen producido a la misma hora al importarlas al agregador. Por ejemplo, en un agregador que agrega datos de husos horarios diferentes, puede ver el inicio de sesión de un registro a las 21:00 con un huso horario original UTC-02:00 y otro registro de inicio de sesión a las 21:00 en un huso horario original UTC-05:00. Esto significa que estos sucesos se produjeron con una diferencia de 3 horas, pero respectivamente en la misma hora (21:00 h).

Entidad Valores de datos cambiados

Esta entidad se utiliza con la solución de réplica IBM InfoSphere Change Data Capture (InfoSphere CDC) que permite la réplica hacia y desde las bases de datos soportadas. Se puede utilizar el mantenimiento de bases de datos replicadas para reducir las sobrecargas y el tráfico de la red.

Los clientes de IBM Guardium con supervisión de actividades de base de datos tendrán acceso a InfoSphere CDC.

Esta característica de Guardium utiliza la salida de usuario de Java CDC para enviar información de cambios de valor al recopilador de Guardium.

Las salidas de usuario para InfoSphere CDC permiten al usuario definir un conjunto de acciones que InfoSphere CDC puede ejecutar antes o después de que se produzca un suceso de base de datos en una tabla especificada.

Tabla 21. Entidad Valores de datos cambiados

Atributo	Descripción
ID SQL completo	Identificador exclusivo para el SQL completo.
Nombre de tabla	Nombre de tabla desde la base de datos
Nombre de columna	Nombre de columna desde la base de datos
Valor antiguo	Valor anterior al cambio.
Valor nuevo	Valor después del cambio.

Atributo	Descripción
Indicación de fecha y hora	Hora en la que se creó el registro.

Es necesario instalar dos archivos en el servidor de base de datos para la comunicación entre el agente de Guardium y la aplicación IBM InfoSphere Change Data Capture (InfoSphere CDC). Se encuentran en el directorio sources/apps/GuardCDC/lib/ de la compilación. Estos archivos son: protobuf-java-2.4.1.jar y GuardCdc.jar.

Instrucciones de instalación

Requisitos previos: la aplicación InfoSphere Change Data Capture (InfoSphere CDC) debe estar ya instalada en el servidor de base de datos.

Pasos para instalar el agente de Guardium en el servidor de bases de datos:

1. Copie estos dos archivos en el directorio RepEngine/lib/ del directorio cdchome. Un ejemplo de la vía de acceso completa sería /cdchome/cdc6.5.2/RepEngine/lib/
2. Descomprima cada archivo
3. Edite el archivo guard_cdc_user_exit_config.mxl para añadir el nombre de Guardium_Host. Un ejemplo de dónde se debe ubicar este archivo sería /cdchome/cdc6.5.2/RepEngine/lib/com/guardium/cdc/userexit/
4. Configure InfoSphere CDC para escribir en GuardiumAgent. Hay varios pasos para preparar y configurar la aplicación CDC. Obtenga estos pasos del equipo de soporte/desarrollo de InfoSphere CDC en IBM.

Entidad Resultados del proceso de clasificación

Esta entidad se crea para cada regla de proceso de clasificación que se desencadena.

Tabla 22. Entidad Resultados del proceso de clasificación

Atributo	Descripción
Catálogo	Ubicación del catálogo para conjuntos de resultados.
Esquema	Nombre de esquema si es aplicable.
Nombre de tabla	Nombre de tabla desde la definición de regla.
Nombre de columna	Nombre de columna desde la definición de regla.
Descripción de regla	Descripción de la regla de política del clasificador.
Comentarios	Comentarios añadidos a esta definición de regla.
Nombre de clasificación	Clasificación para la regla.
Categoría	Categoría para la regla.
Descripción de origen de datos	Origen de datos para la regla.

Entidad Ejecución de proceso de clasificación

Esta entidad describe una ejecución de trabajo de proceso de clasificación.

Tabla 23. Entidad Ejecución de proceso de clasificación

Atributo	Descripción
Descripción de proceso	Desde la definición de proceso.
Estado	Estado del trabajo.
Fecha/hora cola	Indicación de fecha y hora en que el trabajo se sometió a la cola de asesoramiento/clasificación.
Fecha y hora de inicio	Indicación de fecha y hora al inicio del trabajo.
Fecha y hora de finalización	Indicación de fecha y hora al finalizar el trabajo.
Orígenes de datos	Identifica la lista de orígenes de datos para el trabajo.

Entidad Cliente/Servidor

Esta entidad describe una conexión cliente-servidor específica. Se crea una instancia cada vez que se detecta un conjunto exclusivo de atributos (excluida la indicación de fecha y hora).

Tabla 24. Entidad Cliente/Servidor

Atributo	Descripción
ID de acceso	Identificador exclusivo para esta conexión cliente/servidor.
Indicación de fecha y hora	Puesto que todos los atributos de esta entidad contienen información estática, esta indicación de fecha y hora sólo se crea una vez, cuando Guardium observa una solicitud en la conexión de cliente-servidor definida por primera vez.
Fecha de indicación de fecha y hora	Solo fecha desde la indicación de fecha y hora.
Hora de indicación de fecha y hora	Solo hora desde la indicación de fecha y hora.
Día de semana de indicación de fecha y hora	Solo día de la semana desde la indicación de fecha y hora.
Año de indicación de fecha y hora	Solo año desde la indicación de fecha y hora

Atributo	Descripción
Tipo de servidor	DB2, Oracle, Sybase, etc.
IP de cliente	Dirección IP del cliente.
IP de servidor	Dirección IP de servidor.
Protocolo de red	Protocolo de red utilizado (por ejemplo, TCP, UDP, etc. Observe que para K-TAP en Oracle, se podría visualizar como IPC o BEQ)
Protocolo de BD	Protocolo específico para el servidor de bases de datos.
Versión de protocolo de BD	Versión del protocolo de BD.
Nombre usuario de BD	Nombre de usuario de base de datos. El nombre de usuario de BD es la persona que se conecta a la base de datos, ya sea local o remota.
Programa fuente	Programa fuente para la interacción.
MAC cliente	Dirección de hardware del servidor.
Nombre de host del cliente	Nombre de host del cliente.
Nombre de servicio	Nombre de servicio para la interacción. En algunos casos (por ejemplo, con las conexiones de memoria compartida de AIX), el nombre de servicio es un alias que se utiliza hasta que se conecta el servicio real. En estos casos, una vez que el servicio real está conectado, se inicia una nueva sesión - de forma que lo que el usuario interpreta como un único inicio de sesión serán dos inicios de sesión. Con Teradata, el nombre de servicio contiene el valor de ID de host lógico de sesión.
SO de servidor	Sistema operativo del servidor. Con Informix, el sistema operativo puede aparecer como: IEEEM indicando Unix o JDBCIEEEI indicando WindowsDEC indicando DEC Alpha Con Teradata, ya que no hay información directa sobre el sistema operativo del cliente/servidor, se utiliza en su lugar el tipo de formato de datos, que indica cómo se almacenan los datos enteros durante la sesión de base de datos. Esto tiene gran relación con la plataforma que se está utilizando y puede aparecer de la siguiente manera: IBM® MAINFRAME // Formato de datos de sistema principal IBM HONEYWELL MAINFRAME // Formato de datos de sistema principal Honeywell AT&T 3B2 // Formato de datos AT&T 3B2. INTEL 8086 // Formato de datos Intel 8086 (IBM PC o compatible) VAX // Formato de datos VAX AMDAHL // Formato de datos Amdahl
SO de cliente	Sistema operativo del cliente. Con Teradata, ya que no hay información directa sobre el sistema operativo del cliente/servidor, se utiliza en su lugar el tipo de formato de datos, que indica cómo se almacenan los datos enteros durante la sesión de base de datos. Esto tiene gran relación con la plataforma que se está utilizando y puede aparecer de la siguiente manera: IBM MAINFRAME // Formato de datos de sistema principal IBM HONEYWELL MAINFRAME // Formato de datos de sistema principal Honeywell AT&T 3B2 // Formato de datos AT&T 3B2. INTEL 8086 // Formato de datos Intel 8086 (IBM PC o compatible) VAX // Formato de datos VAX AMDAHL // Formato de datos Amdahl
Usuario de SO	Cuenta de usuario de SO para la interacción.
Nombre de host del servidor	Nombre de host del servidor.
Descripción del servidor	Descripción del servidor (si la hay).
IP cliente/Usuario BD	Valor de atributo emparejado que consta de la dirección IP del cliente y el nombre de usuario de la base de datos.
IP de cliente analizado	Sólo se aplica al tráfico cifrado; cuando se establece, la dirección IP del cliente se establece en ceros. La dirección IP del cliente analizado está correlacionado con el origen de CEF. Si la consulta utilizada para CEF NO contiene la dirección IP del cliente pero contiene la dirección IP del cliente analizado, se utilizará para el origen la dirección IP del cliente analizado. Si se incluyen ambas en la consulta, la dirección IP del cliente prevalece.
IP Servidor/Usuario BD	Valor de atributo emparejado que consta de la dirección IP del servidor y el nombre de usuario de la base de datos.
Cliente/ Servidor por sesión	Cliente/Servidor por sesión es también una entidad principal. Acceda a esta entidad secundaria pulsando en la entidad primaria Cliente/Servidor.

El ID de acceso solo está disponible a los usuarios con el rol de administrador.

Nota: Sólo para Seguimiento de acceso, el nombre de entidad Cliente/Servidor aparecerá en el menú desplegable como dos entidades posibles: Cliente/Servidor y Cliente/Servidor por sesión.

Cliente/Servidor por sesión recontará desde Cliente/Servidor y condiciones de fecha desde sesión.

Cliente/Servidor recontará desde Cliente/Server y condiciones de fecha también desde Cliente/Servidor.

Si el usuario elige Cliente/Servidor, la consulta se cumplimentará con ATTRIBUTE_ID = 1. Si el usuario elige Cliente/Servidor por sesión, entonces la consulta se cumplimentará con MAIN_ATTRIBUTE_ID = 0.

Entidad Supervisor de uso de almacenamiento intermedio de CM

En el Gestor central, muestra la agregación de todas las entidades Uso de almacenamiento intermedio de sniffer que se han subido.

Tabla 25. Entidad Supervisor de uso de almacenamiento intermedio de CM

Atributo	Descripción
ID de uso de almacenamiento intermedio de sniffer	
Indicación de fecha y hora	Hora en la que se creó el registro.
Porcentaje CPU de sniffer	Porcentaje de CPU utilizado por el sniffer.
Porcentaje memoria de sniffer	Porcentaje de memoria utilizada por el sniffer.
Porcentaje CPU de MySQL	Porcentaje de CPU utilizado por MySQL.
Porcentaje memoria de MySQL	Porcentaje de memoria utilizada por MySQL.
PID	Identificador de proceso de sniffer.
Memoria	Cantidad de memoria utilizada por el sniffer.
Hora	Tiempo transcurrido utilizado por el sniffer.
Almacenamiento intermedio libre	Cantidad de espacio de almacenamiento intermedio libre.
Velocidad analizador	Velocidad a la que se analizan los mensajes.
Cola de analizador	Tamaño de la cola de análisis.
Total analizador	Número total de mensajes analizados.
Cola de registrador	Tamaño de la cola del registrador.
Total de registrador	Número total de mensajes registrados.
Cola de sesión	Tamaño de la cola de sesión.
Total sesión	Número total de sesiones.
Datos de manejador	Datos de motor de procesos de sniffer internos.
STR adicional	Datos de motor de procesos de sniffer internos.
Conexiones utilizadas de sniffer	Número total de conexiones que se están supervisando actualmente desde que se reinició el motor de inspección.
Paquetes de sniffer descartados	Paquetes descartados por el sniffer.
Paquetes ignorados de sniffer	Paquetes ignorados por el empleado.
Paquetes de sniffer regulados	Número total de conexiones que se han ignorado debido a la regulación desde que se reinició el motor de inspección.
Conexiones finalizadas de sniffer	Número total de conexiones que se supervisaron y finalizaron desde que se reinició el motor de inspección.
Recuento de sesiones de registrador	Recuento de sesiones registradas.
Paquetes de registrador ignorados por regla	Paquetes ignorados por la acción de la regla de política.
Paquetes perdidos de analizador	Paquetes perdidos por el analizador.
Bases de datos supervisadas de registrador	Lista de tipos de base de datos que se están supervisando actualmente.
Mysql activo	Indicador booleano de reinicio de base de datos interna (1=se reinició, 0=no se reinició).
Carga de CPU del sistema	Utilización de CPU del sistema.
Tiempo de actividad de sistema	Tiempo desde el último arranque.
Uso de disco de Mysql	Uso de disco de MySQL.
Uso de memoria de sistema	Utilización de memoria del sistema.
Uso del disco Var del sistema	Utilización de disco var del sistema.
Uso de disco raíz de sistema	Utilización de disco raíz del sistema.
Eth0 recibido	Mensajes recibidos en ETH 0.
Eth0 enviado	Mensajes enviados en ETH 0.
Recibidos modalidad promiscua	Ratio de paquetes recibidos a través de las tarjetas de red para sniffer (puertos que no son de interfaz).

Atributo	Descripción
FD abiertos	Descriptores de archivo abiertos.
FD abiertos de MySQL	Descriptores de archivo abiertos de base de datos
Sesiones normales	Recuento de sesiones normales.
Sesiones no abiertas	Recuento de sesiones no abiertas por el sniffer.
Tiempo de espera de sesión	Número de sesiones que han excedido el tiempo de espera.
Sesiones ignoradas	Recuento de sesiones ignoradas por el sniffer.
Sesiones cerradas directamente	Recuento de sesiones cerradas directamente.
Sesiones adivinadas	Recuento de sesiones adivinadas.
Indicación de fecha y hora de SqlGuard	Momento en que el registro se inserta en la tabla personalizada
Nombre de origen de datos	Es el nombre del origen de datos utilizado para subir el registro

Entidad Mandato

Para cada mandato, se crea una entidad para cada nodo padre y posición en la que el mandato aparece en una construcción de mandato.

Tabla 26. Entidad Mandato

Atributo	Descripción
ID de mandato	Identifica el mandato de forma exclusiva.
ID de construcción	Identifica de forma exclusiva la construcción (por ejemplo, select a from b).
Verbo SQL	Verbo principal en el mandato SQL (por ejemplo, select, insert, delete, etc.).
Profundidad	Profundidad del mandato en el árbol de análisis de SQL.
Padre	Identificador del nodo padre en el árbol de análisis.

El ID de mandato y el ID de construcción sólo están disponibles a los usuarios con el rol de administrador.

Entidad Comentarios

Esta entidad describe un comentario de usuario. Sólo está disponible en el dominio de Comentarios, que está restringido a los usuarios administradores. Este dominio sólo incluye comentarios que se pueden compartir, que son todos los comentarios, excepto aquellos que se ejecutan localmente (consulte la entidad Comentarios locales).

Tabla 27. Entidad Comentarios

Atributo	Descripción
Creador de comentario	Usuario de Guardium que creó el comentario.
Referencia de comentario	Indica el elemento al que se adjunta el comentario - una consulta, un resultado del proceso de auditoría u otro comentario, por ejemplo.
Contenido de comentario	El texto completo del comentario.
Indicación de fecha y hora	Fecha y hora en que se creó el comentario.
Año de indicación de fecha y hora	Solo año desde la indicación de fecha y hora
Día de semana de indicación de fecha y hora	Solo día de la semana desde la indicación de fecha y hora.
Hora de indicación de fecha y hora	Solo hora desde la indicación de fecha y hora.
Fecha de indicación de fecha y hora	Solo fecha desde la indicación de fecha y hora.
Descripción de objeto	Nombre del objeto desde el que se ha definido el comentario. Por ejemplo, un comentario definido en una política tiene una descripción de objeto de ACCESS_RULE_SET.
Asociaciones de registro	Una lista de registros a los que está asociado este comentario.

Entidad Texto de error de base de datos

El texto de cada mensaje de error de base de datos común se almacena en una tabla de la base de datos interna de Guardium. Está disponible sólo para crear informes desde la entidad Excepción propietaria para cada excepción que es un error de base de datos. Algunos tipos de excepciones, por ejemplo, las conexiones o reconexiones de S-TAP, no tienen textos de error de base de datos.

Tabla 28. Entidad Texto de error de base de datos

Atributo	Descripción
Texto de error de base de datos	Código de error de base de datos seguido de una descripción de texto breve del error. El código de error se toma del atributo Descripción de excepción de la entidad Excepción. Utilizando el código de error como clave, el texto de error se obtiene de una tabla interna en el dispositivo Guardium, que contiene los mensajes de error más comunes (unos 54,000 de ellos). Por ejemplo: ORA-00942: table or view does not exist

Atributo	Descripción
Código de error	Muestra el código de error de la base de datos.

Entidad Origen de datos

Esta entidad (bajo la Entidad Seguimiento de la config. de CAS / Detalles de elemento supervisado) identifica un origen de datos.

Tabla 29. Entidad Origen de datos

Atributo	Descripción
ID de origen de datos	Identifica un conjunto de resultados para un origen de datos
Tipo de origen de datos	Tipo de origen de datos: Oracle, MS-SQL, DB2, Sybase, Informix, etc.
Nombre de origen de datos	Nombre de origen de datos
Descripción de origen de datos	Descripción del origen de datos
Host	Nombre de host del origen de datos
Puerto	Número de puerto en el host
Nombre de servicio	Nombre de servicio para el origen de datos
Nombre de usuario	Nombre de usuario para el acceso al origen de datos
Nombre de base de datos	Nombre de base de datos
Último comentario	Último comentario
Compartido	Sí o No
Propiedades de conexión	El recuadro Propiedad de conexión contiene información sobre la misma solo si se deben incluir propiedades de conexión adicionales en el URL de JDBC para establecer una conexión JDBC con este origen de datos.

Entidad Host descubierto

Esta entidad identifica un host descubierto.

Tabla 30. Entidad Host descubierto

Atributo	Descripción
IP de servidor	Dirección IP del host descubierto.
Nombre de host del servidor	Nombre del host descubierto.
Huso horario original	Desplazamiento de UTC. Esto se realiza en concreto para los agregadores que tienen recopiladores en distintos husos horarios y, por lo tanto, actividades que se han realizado en distintas horas no parecen como si se hubiesen producido a la misma hora al importarlas al agregador. Por ejemplo, en un agregador que agrega datos de husos horarios diferentes, puede ver el inicio de sesión de un registro a las 21:00 con un huso horario original UTC-02:00 y otro registro de inicio de sesión a las 21:00 en un huso horario original UTC-05:00. Esto significa que estos sucesos se produjeron con una diferencia de 3 horas, pero respectivamente en la misma hora (21:00 h).

Entidad Instancias descubiertas

Esta entidad identifica las instancias descubiertas.

Tabla 31. Entidad Instancias descubiertas

Atributo	Descripción
Indicación de fecha y hora	Valor de indicación de fecha y hora creado cuando Guardium graba esta instancia de la entidad (cada instancia tiene una indicación de fecha y hora exclusiva).
Host	Nombre de host para esta instancia
Protocolo	Protocolo específico de esta instancia
Mínimo puerto	Rango de puertos, número de puerto mínimo para los motores de inspección
Máx. de puerto	Rango de puertos, número de puerto máximo para los motores de inspección
IP de cliente	Dirección IP/máscara del cliente
Excluir IP de cliente	Dirección IP/máscara de clientes a excluir
Nombres proc	Nombre del ejecutable de la base de datos
Conducto con nombre	Nombre de conducto con nombre utilizado por la base de datos
Puerto BD KTAP	Puerto de base de datos para KTAP
Dir instalación BD	Directorio de instalación de base de datos
Nombre proc	Nombre de proceso
Ajuste mem compartida DB2	Tamaño de cabecera de paquete
Posición cliente mem compartida DB2	Desplazamiento de áreas de E/S de cliente
Tamaño mem compartida DB2	Tamaño segmento memoria compartida DB2

Atributo	Descripción
Nombre de instancia	Nombre de la instancia descubierta
Versión de Informix	Versión de Informix

Entidad Puerto descubierto

Esta entidad identifica un puerto descubierto.

Tabla 32. Entidad Puerto descubierto

Atributo	Descripción
Puerto	Número de puerto descubierto.
Sondeo intentado	Indica si se ha intentado un sondeo para un servicio de base de datos soportado en este puerto. T=sí, F=no.
Tipo de puerto	Indica el tipo de puerto (normalmente TCP).
Tipo de BD	Si un sondeo del puerto encuentra un tipo de base de datos soportado, indica el tipo (DB2, Informix, MS SQL Server, etc.)
Indicación de fecha y hora de sondeo	Fecha y hora en que se ha sondeado este puerto específico.
Huso horario original	Desplazamiento de UTC. Esto se realiza en concreto para los agregadores que tienen recopiladores en distintos husos horarios y, por lo tanto, actividades que se han realizado en distintas horas no parecen como si se hubiesen producido a la misma hora al importarlas al agregador. Por ejemplo, en un agregador que agrega datos de husos horarios diferentes, puede ver el inicio de sesión de un registro a las 21:00 con un huso horario original UTC-02:00 y otro registro de inicio de sesión a las 21:00 en un huso horario original UTC-05:00. Esto significa que estos sucesos se produjeron con una diferencia de 3 horas, pero respectivamente en la misma hora (21:00 h).

Entidad Excepción

Esta entidad se crea para cada excepción encontrada.

Tabla 33. Entidad Excepción

Atributo	Descripción
ID de excepción	Identifica la excepción de forma exclusiva.
Id de tipo de excepción	Identifica el tipo de excepción de forma exclusiva.
Indicación de fecha y hora de excepción	Fecha y hora en la que se registró la entidad Excepción.
Fecha de excepción	Solo fecha desde la indicación de fecha y hora.
Tiempo de excepción	Solo hora desde la indicación de fecha y hora.
Día de la semana de la excepción	Solo día de la semana desde la indicación de fecha y hora.
Año de excepción	Solo año desde la indicación de fecha y hora
Dirección de origen	Dirección IP de origen de la excepción.
Puerto de origen	Número de puerto de origen.
Dirección de destino	Dirección IP de destino.
Puerto de destino	Número de puerto de destino.
Protocolo de base de datos	Protocolo de base de datos para la excepción.
Nuevo valor TTL	Reservado para ser utilizado únicamente por el rol de administrador.
Descripción de excepción	Descripción de la excepción. Para una excepción de reconexión o tiempo de espera excedido de S-TAP, contendrá la dirección IP o el nombre DNS del servidor de bases de datos. Para una excepción de base de datos, se trata de un código de error procedente del sistema de gestión de bases de datos. Para la mayoría de los mensajes comunes (alrededor de 54,000 de ellos), hay disponible una descripción de texto extensa en el atributo Texto de error de base de datos. Dicho texto procede de la tabla interna de base de datos de Guardium de mensajes de error, no de la propia excepción.
Serie SQL que causó la excepción	La serie SQL que ha causado la excepción.
Nombre de usuario	Nombre de usuario de base de datos. En el tráfico cifrado, donde es necesario la correlación, es posible que este valor no esté disponible, pero siempre está disponible desde el atributo Nombre de usuario de BD en la entidad Cliente/Servidor.
Nombre de usuario de aplicación	Nombre del usuario de la aplicación.
Enlace a más información sobre la excepción1	Enlace opcional que a veces está disponible, en función del origen de excepción.
ID1 global	Identificador global de la excepción.

Atributo	Descripción
Huso horario original	Desplazamiento de UTC. Esto se realiza en concreto para los agregadores que tienen recopiladores en distintos husos horarios y, por lo tanto, actividades que se han realizado en distintas horas no parecen como si se hubiesen producido a la misma hora al importarlas al agregador. Por ejemplo, en un agregador que agrega datos de husos horarios diferentes, puede ver el inicio de sesión de un registro a las 21:00 con un huso horario original UTC-02:00 y otro registro de inicio de sesión a las 21:00 en un huso horario original UTC-05:00. Esto significa que estos sucesos se produjeron con una diferencia de 3 horas, pero respectivamente en la misma hora (21:00 h).

El ID de excepción y el ID de tipo de excepción sólo están disponibles a los usuarios con el rol de administrador.

Entidad Tipo de excepción

Hay un conjunto fijo de tipos de excepción, uno de los cuales se asociará a cada excepción registrada. Estos tipos están disponibles sólo para informes de la entidad Excepción propietaria.

Tabla 34. Entidad Tipo de excepción

Atributo	Descripción
Descripción de excepción	Descripción de texto del tipo de excepción, de la lista siguiente. La mayoría de ellas nunca deberían darse. Consulte las notas en cursiva para ver las notas y excepciones más comunes. Se ha utilizado una nueva construcción El proceso de alerta ha generado una excepción Excepción de proceso de alertas personalizadas El servidor de bases de datos ha devuelto un error Para este mensaje, se almacenará un código de error de base de datos en el atributo Descripción de excepción de la entidad Excepción, y una versión de texto del mensaje de error de base de datos estará disponible en el atributo Texto de error de base de datos de la entidad Texto de error de base de datos. Excepción de protocolo de BD Impresiones de depuración a través del mecanismo de EXCEPTION Solicitudes descartadas de la base de datos La información de sesión se ha descartado debido a un tráfico excesivo. Error durante el proceso del sistema de auditoría de configuración Error durante el proceso de clasificación Invocación de consulta no válida Error de inicio de sesión Excepción del protocolo de BD de bajo nivel El trabajo planificado ha arrojado una excepción Excepción del asesoramiento de seguridad Excepción de seguridad Para este mensaje, se genera una excepción de clase personalizada cuando se bloquea la ejecución del código ilegítimo; como cuando los usuarios utilizan la API de Java™ para definir sus propias alertas o asesoramientos. Se ha cerrado la sesión de forma prematura Excepción del analizador de SQL Reconexión de la conectividad de S-TAP Para este mensaje, la dirección IP o el nombre DNS del servidor de bases de datos estará disponible en el atributo Descripción de excepción de la entidad Excepción Tiempo de espera excedido de la conectividad de S-TAP Para este mensaje, la dirección IP o el nombre DNS del servidor de bases de datos estará disponible en el atributo Descripción de excepción de la entidad Excepción ERROR DE TCP Para este mensaje, se incluirá información adicional sobre el error en el atributo Descripción de excepción de la entidad Excepción La clase Turbine ha arrojado una excepción No se ha podido depurar el informe

Entidad Campo

Cada vez que Guardium se encuentra con un nuevo campo, crea una entidad Campo.

Tabla 35. Entidad Campo

Atributo	Descripción
ID de campo	Identifica el campo de forma exclusiva.
ID de construcción	Identifica de forma exclusiva la construcción en la que se ha referenciado.
ID de mandato	Identifica de forma exclusiva el mandato principal desde la construcción en la que ha sido referenciado.
ID de objeto	Identifica de forma exclusiva el objeto desde la construcción en la que ha sido referenciado.
Nombre de campo	Nombre del campo.
Cláusula List Cláusula Where Cláusula Order by Cláusula Having Cláusula Group By Cláusula On	Utilice estos atributos para ordenar consultas SQL complejas. Ejemplo de consultas SQL: Order by SELECT * FROM dept_costs WHERE dept_total > (SELECT avg FROM avg_cost) ORDER BY department Having SELECT column_name1, SUM(column_name2) FROM table_name GROUP BY column_name1 HAVING (numerical function condition) Group By SELECT column_name1, SUM(column_name2) FROM table_name GROUP BY column_name1 Where SELECT FirstName, LastName, City FROM Users WHERE City = Los Angeles

ID de campo, ID de construcción, ID de mandato e ID de objeto solo están disponibles a los usuarios con el rol de administrador.

Entidad Valor de campo SQL

Estas entidades sólo se crean mediante acciones de regla de política que se registran con valores; por ejemplo: Registrar todos los detalles con valores y Registrar todos los detalles por sesión con valores. El valor del campo registrado puede estar opcionalmente asociado a un nombre de campo. Por ejemplo, los nombres de campo estarán disponibles (en la entidad Campo) si se registra la sentencia siguiente:

insert into t1 (foo, bar) (10, 20)

Pero no estarán disponibles cuando se registre la siguiente sentencia:

insert into t2 (10, 20)

Tabla 36. Entidad Valor de campo SQL

Atributo	Descripción
Valor	Valor de campo de la construcción registrada.

Entidad Flat Log

Esta entidad describe la actividad de proceso de Flat Log.

Tabla 37. Entidad Flat Log

Atributo	Descripción
SQL completo	El SQL completo registrado.
Indicación de fecha y hora	Indicación de fecha y hora en la que se inició la sesión.
Fecha de indicación de fecha y hora	Parte de la fecha de la indicación de fecha y hora.

Atributo	Descripción
Hora de indicación de fecha y hora	Parte de la hora de la indicación de fecha y hora.
Tiempo de respuesta	Tiempo de respuesta de la solicitud en milisegundos.
Registros afectados	Número de registros afectados por la solicitud.
Satisfactorio	Indica si la solicitud ha sido satisfactoria (True/False).
Tipo de sentencia	Tipo de sentencia SQL SQL: simple, mandato SQL directo, por ejemplo, escrito directamente en la CLI RAW: PREPARE de una sentencia SQL para una posterior ejecución, por ejemplo, conn.prepareStatement (select a from b where c=:value) BIND: ejecución de una sentencia preparada que incluye valores de parámetro de vinculación El tipo de sentencia forma parte de la entidad SQL FULL y sólo se audita si se ha configurado Detalles completos de registro para esta sentencia dentro de la política. No es posible filtrar tipos de sentencia específicos en la política, por ejemplo, sentencias BIND y SQL sólo de auditoría. Sin embargo, puede filtrarlos en informes.
Datos devueltos	Datos devueltos (si hay)
Información de vinculación	Información de vinculación para la solicitud
Valores de variables de vincular	Con DB2/zOS, contiene una lista separada de comas de variables de vinculación
Huso horario original	Desplazamiento de UTC. Esto se realiza en concreto para los agregadores que tienen recopiladores en distintos husos horarios y, por lo tanto, actividades que se han realizado en distintas horas no parecen como si se hubiesen producido a la misma hora al importarlas al agregador. Por ejemplo, en un agregador que agrega datos de husos horarios diferentes, puede ver el inicio de sesión de un registro a las 21:00 con un huso horario original UTC-02:00 y otro registro de inicio de sesión a las 21:00 en un huso horario original UTC-05:00. Esto significa que estos sucesos se produjeron con una diferencia de 3 horas, pero respectivamente en la misma hora (21:00 h).

Entidad SQL completo

Las entidades SQL completo únicamente las crean las siguientes acciones de regla de política: Registrar todos los detalles, Registrar todos los detalles con valores, Registrar todos los detalles por sesión o Registrar todos los detalles por sesión con valores.

Tabla 38. Entidad SQL completo

Atributo	Descripción
SQL completo	Sentencia SQL completa que incluye valores.
Indicación de fecha y hora	Indicación de fecha y hora que registra cuándo se ha ejecutado el SQL en el servidor de bases de datos.
Tiempo de respuesta	Tiempo de respuesta de la solicitud en milisegundos. Cuando las solicitudes se supervisan en el tráfico de red, los tiempos de respuesta son un reflejo preciso del tiempo que se tarda en responder a la solicitud (Guardium registra las indicaciones de fecha y hora tanto de la solicitud del cliente como de la respuesta del servidor).
Registros afectados	Número de registros afectados por cada sesión. En informes que utilizan este atributo, sugerimos que active los alias para visualizar casos especiales de forma adecuada, por ejemplo, Conjunto de resultados grande o N/D.
Datos devueltos	Datos devueltos para esta solicitud (si hay alguna, y si están disponibles).
ID SQL completo	Identificador exclusivo para el SQL completo.
ID de instancia	Identificador exclusivo para la instancia de SQL completo.
Satisfactorio	Indica si la llamada ha sido satisfactoria.
Registros afectados (Desc)	Cuando el valor de Registros afectados es un valor de una serie en lugar de un número, dicha serie se almacena aquí. Por ejemplo: Conjunto de resultados grande o N/D.
Descripción de regla de acceso	Descripción de la regla de política utilizada
Recuento de datos devueltos	Número de filas devueltas de la sentencia SQL utilizada en la regla de política.
Confirmación automática	Las entradas se numeran automáticamente.
Tiempo de respuesta de acuse de recibo	Tiempo de acuse de recibo en milisegundos.
Recuento de kbytes en entrada (Ingress)	Registra el número de bytes en solicitudes.
Recuento de kbytes en salida (Egress)	Registra el número de bytes en respuestas.

Atributo	Descripción
Tipo de sentencia	Tipo de sentencia SQL SQL: simple, mandato SQL directo, por ejemplo, escrito directamente en la CLI RAW: PREPARE de una sentencia SQL para una posterior ejecución, por ejemplo, conn.prepareStatement (select a from b where c=:value) BIND: ejecución de una sentencia preparada que incluye valores de parámetro de vinculación El tipo de sentencia forma parte de la entidad SQL FULL y sólo se audita si se ha configurado Detalles completos de registro para esta sentencia dentro de la política. No es posible filtrar tipos de sentencia específicos en la política, por ejemplo, sentencias BIND y SQL sólo de auditoría. Sin embargo, puede filtrarlos en informes.
Valores de variables de vincular	Con DB2/zOS, contiene una lista separada de comas de variables de vinculación
Huso horario original	Desplazamiento de UTC. Esto se realiza en concreto para los agregadores que tienen recopiladores en distintos husos horarios y, por lo tanto, actividades que se han realizado en distintas horas no parecen como si se hubiesen producido a la misma hora al importarlas al agregador. Por ejemplo, en un agregador que agrega datos de husos horarios diferentes, puede ver el inicio de sesión de un registro a las 21:00 con un huso horario original UTC-02:00 y otro registro de inicio de sesión a las 21:00 en un huso horario original UTC-05:00. Esto significa que estos sucesos se produjeron con una diferencia de 3 horas, pero respectivamente en la misma hora (21:00 h).

ID SQL completo, ID de instancia y Satisfactorio solo están disponibles a los usuarios con el rol de administrador.

Entidad Valores de SQL completo

Estas entidades sólo mediante las siguientes acciones de regla de política: Registrar todos los detalles con valores y Registrar todos los detalles por sesión con valores.

Tabla 39. Entidad Valores de SQL completo

Atributo	Descripción
Valores	Uno o varios valores desde la construcción registrada.
Indicación de fecha y hora	Fecha y hora en la que se creó la entidad Valores SQL completo.

Entidad Sucesos de GIM

Esta entidad describe sucesos que se han producido mientras se utilizaba Guardium Installation Manager (GIM).

Tabla 40. Entidad Sucesos de GIM

Atributo	Descripción
Generador de suceso	Dirección IP del cliente (es decir, servidor de BD) que ha generado el suceso.
Descripción de suceso	Descripción de suceso.
Hora de suceso	Hora en la que se ha producido el suceso.

Entidad Grupo

Esta entidad describe un grupo definido para Guardium.

Tabla 41. Entidad Grupo

Atributo	Descripción
Descripción de grupo	Nombre del grupo.
Subtipo de grupo	Subtipo, si lo hay, definido para el grupo.
Indicación de fecha y hora	Fecha y hora en que se creó la entidad de grupo.

Entidad Miembro de grupo

Esta entidad describe un grupo definido para Guardium.

Tabla 42. Entidad Miembro de grupo

Atributo	Descripción
Miembro de grupo	Nombre del miembro del grupo.
Indicación de fecha y hora	Fecha y hora en que se creó o actualizó el miembro del grupo.
Fecha de indicación de fecha y hora	Solo fecha desde la indicación de fecha y hora.
Hora de indicación de fecha y hora	Solo hora desde la indicación de fecha y hora.
Año de indicación de fecha y hora	Solo año desde la indicación de fecha y hora

Atributo	Descripción
Día de semana de indicación de fecha y hora	Solo día de la semana desde la indicación de fecha y hora.

Entidad Tipo de grupo

Esta entidad describe un tipo de grupo de Guardium (usuario, dirección IP de cliente, mandato, etc.).

Tabla 43. Entidad Tipo de grupo

Atributo	Descripción
Tipo de grupo	Identifica el tipo de grupo.
Indicación de fecha y hora	Fecha y hora en que se creó el tipo de grupo.

Tipos de actividad de Guardium

Esta entidad describe las distintas actividades de usuario

Tabla 44. Tipos de actividad de Guardium

Atributo	Descripción
Descripción de tipo de actividad	Descripción de la actividad
ID de tipo de actividad	Identifica de forma exclusiva el tipo de actividad.

Entidad Rol de Guardium

Esta entidad (bajo la entidad Usuario) identifica un rol de Guardium.

Tabla 45. Entidad Rol de Guardium

Atributo	Descripción
Identificador de rol	ID de rol identificado.
Rol	Rol de Guardium listado.

Entidad Aplicaciones de Guardium

Esta entidad (bajo la entidad Usuario) identifica una aplicación de Guardium.

Tabla 46. Entidad Aplicaciones de Guardium

Atributo	Descripción
Identificador de aplicación	ID de aplicación identificado.
Aplicación	Aplicación de Guardium listada (por ejemplo, Creador de consultas, Creador de políticas, etc.).

Entidad Tipos de actividad de Guardium

Se define una instancia en la base de datos interna de Guardium para cada tipo de actividad.

Tabla 47. Entidad Tipos de actividad de Guardium

Atributo	Descripción
Descripción de tipos de actividad	Descripción de una actividad.

Entidad Auditoría de actividad de usuario de Guardium

Esta entidad se crea para cada actividad de usuario de Guardium.

Tabla 48. Entidad Auditoría de actividad de usuario de Guardium

Atributo	Descripción
ID de inicio de sesión	ID utilizado para el inicio de sesión.
Nombre de usuario	Nombre de usuario de Guardium para la actividad.
Indicación de fecha y hora	Se crea al registrar la actividad.
Entidad modificada	Entidad de Guardium modificada (por ejemplo, una definición de grupo).
Clave de entidad utilizada	Clave utilizada para acceder a la entidad.
Valor clave	Valor nuevo de la entidad.
Todos los valores	Todos los valores modificados.
Descripción de objeto	Nombre del objeto específico modificado.
ID global	ID global exclusivo para la sesión.
Nombre de host	Nombre de host del usuario.

Entidad Inicio de sesión de usuarios de Guardium

Esta entidad se crea cada vez que un usuario inicia una sesión en el dispositivo Guardium.

Tabla 49. Entidad Inicio de sesión de usuarios de Guardium

Atributo	Descripción
ID de inicio de sesión	ID utilizado para el inicio de sesión.
Nombre de usuario	Se crea cuando el usuario de Guardium inicia o finaliza la sesión (habrá una entidad por cada sesión de Guardium).
Fecha y hora de inicio de sesión	Fecha y hora en que el usuario inició la sesión.
Fecha y hora de finalización de sesión	Fecha y hora en que el usuario finalizó la sesión.
Inicio de sesión satisfactorio	Indica si el inicio de sesión fue satisfactorio.
ID global	ID global exclusivo para la sesión.
Nombre de host	Nombre de host del usuario.
Dirección remota	Dirección remota del usuario.

Entidad Host

Se crea una entidad Host de CAS la primera vez que se detecta CAS en un host de servidor de base de datos. Se actualiza cada vez que cambia el estado en línea/fuera de línea. La entidad Host también está disponible en el dominio Historial de host de CAS.

Tabla 50. Entidad Host

Atributo	Descripción
Nombre de host	Nombre de host del servidor de bases de datos (se puede mostrar como una dirección IP)
Tipo de SO	Sistema operativo: UNIX o WIN
Está en línea	Estado en línea (Sí/No) cuando se escribió el registro
ID de host	Identifica el registro de host

Entidad Configuración de host

Se crea una entidad Configuración de host para cada elemento en una instancia de CAS.

Tabla 51. Entidad Configuración de host

Atributo	Descripción
ID de etiqueta de estado de auditoría	Identificador numérico exclusivo para el elemento de configuración
Indicación de fecha y hora	Indicación de fecha y hora para la creación de la entidad
Nombre de host	Nombre de host o dirección IP del servidor de bases de datos
Tipo de SO	Sistema operativo: UNIX o Windows.
Tipo de BD	Tipo de base de datos: Oracle, MS-SQL, DB2, Sybase, Informix o N/D si el cambio es para una instancia de sistema operativo
Nombre de instancia	Nombre de la instancia del conjunto de plantillas
Tipo	Tipo de elemento supervisado que ha cambiado. Script de SO o Script SQL: Cambio desencadenado por el script de SO contenido en la definición de plantilla de elemento supervisado. Variable de entorno: una variable de entorno (sólo Unix) Variable de registro: una variable de registro (sólo Windows) Archivo: un archivo específico. No hay ninguna entidad de configuración de host para un patrón de archivo definido en el conjunto de plantillas utilizado por la instancia. En su lugar, hay una entidad de configuración de host distinta para cada archivo que coincide con el patrón.
Elemento supervisado	Nombre del elemento modificado, de la Descripción (si se ha especificado), de lo contrario, es un nombre predeterminado que depende del tipo (un nombre de archivo, por ejemplo).

Entidad Suceso de host

Se crea un suceso de host cada vez que CAS detecta o señaliza un suceso (consulte los tipos de suceso).

Tabla 52. Entidad Suceso de host

Atributo	Descripción
ID de suceso de host de auditoría	Identifica la entidad de suceso de host
Hora de suceso	Fecha y hora en que se registró el suceso

Atributo	Descripción
Tipo de suceso	Identifica el suceso que se está registrando: Cliente activo - CAS iniciado en el host de servidor de base de datos Cliente inactivo - CAS detenido en el host de servidor de base de datos Sustitución por anomalía inactiva - Hay disponible un servidor (a seguir a una interrupción), de forma que los datos de CAS se están escribiendo en el servidor Sustitución por anomalía activa - El servidor no está disponible por lo que los datos de CAS se están escribiendo en el archivo de sustitución por anomalía Servidor inactivo - El servidor de bases de datos está detenido Servidor activo - El servidor de bases de datos está iniciado
Indicación de fecha y hora	Indicación de fecha y hora para la creación de la entidad
ID de host de auditoría	Identifica el host
Huso horario original	Desplazamiento de UTC. Esto se realiza en concreto para los agregadores que tienen recopiladores en distintos husos horarios y, por lo tanto, actividades que se han realizado en distintas horas no parecen como si se hubiesen producido a la misma hora al importarlas al agregador. Por ejemplo, en un agregador que agrega datos de husos horarios diferentes, puede ver el inicio de sesión de un registro a las 21:00 con un huso horario original UTC-02:00 y otro registro de inicio de sesión a las 21:00 en un huso horario original UTC-05:00. Esto significa que estos sucesos se produjeron con una diferencia de 3 horas, pero respectivamente en la misma hora (21:00 h).

Entidad Incidencia

Las entidades de incidencia se crean con los procesos de generación de incidencias, o manualmente mediante la asignación de una infracción de política para una incidencia.

Tabla 53. Entidad Incidencia

Atributo	Descripción
Indicación de fecha y hora	Hora en la que se creó la incidencia.
Nombre de categoría	Categoría asignada a la incidencia.
Número de incidencia	Número de incidencia (asignado secuencialmente).

Entidad Gravedad de incidencia

Descripción de la gravedad de una incidencia.

Tabla 54. Entidad Gravedad de incidencia

Atributo	Descripción
Descripción de gravedad de incidencia	El código de gravedad será uno de los siguientes: INFORMACIÓN, BAJA, MEDIA, ALTA

Entidad Estado de incidencia

Describe el estado de una entidad de Incidencia.

Tabla 55. Entidad Estado de incidencia

Atributo	Descripción
Descripción de estado	Será uno de los valores siguientes: ABIERTA - La incidencia todavía no se ha asignado a un usuario. ASIGNADA - Se ha asignado la incidencia. CERRADA - La incidencia está cerrada.

Entidad Política instalada

Describe la política instalada.

Tabla 56. Entidad Política instalada

Atributo	Descripción
ID	Identifica el registro de instalación de política.
ID de conjunto de reglas	Identifica el conjunto de reglas.
Descripción de política	Descripción desde la definición de política.
Seguimiento de auditoría selectivo	Indica si se trata de una política de seguimiento de auditoría selectiva (verdadero/falso).
Patrón de auditoría	Patrón de prueba utilizado para una política de seguimiento de auditoría selectiva.

Atributo	Descripción
Indicación de fecha y hora	Indicación de fecha y hora de la creación del registro.
Secuencia	Establece el orden de la secuencia cuando hay varias políticas instaladas.

Entidad Configuración de instancia

Se crea una entidad de configuración de instancia cada vez que se define una configuración de instancia. Esta entidad define cómo se conecta la instancia de CAS a la base de datos (si es necesario) e identifica el conjunto de plantillas utilizado por la instancia. Proporciona el estado actual de la última instancia (en uso, habilitada o inhabilitada) y la fecha de la última revisión.

Atributos de entidad Configuración de instancia

Tabla 57. Entidad Configuración de instancia

Atributo	Descripción
ID de configuración	Identifica este registro de configuración.
Indicación de fecha y hora	Indicación de fecha y hora del registro creado.
Tipo de BD	Tipo de base de datos: Oracle, MS-SQL, DB2, Sybase, Informix o N/D para una instancia de sistema operativo
Instancia	Nombre de la instancia.
Usuario	Nombre de usuario que CAS utiliza para iniciar una sesión en la base de datos o N/D para una instancia de sistema operativo.
Puerto	Número de puerto que CAS utiliza para conectarse a la base de datos; o vacío para una instancia de sistema operativo
Directorio inicio BD	Directorio de inicio para la base de datos; o vacío para una instancia de sistema operativo
ID de conjunto de plantillas	Identifica el conjunto de plantillas utilizado por esta instancia
Tipo de SO	Sistema operativo del host: UNIX o Windows

Entidad Unión

Una tabla de unión es una forma de implementar relaciones de muchos a muchos. Utilice la entidad Unión para unir tablas en una sentencia SQL SELECT.

Tabla 58. Entidad Unión

Atributo	Descripción
ID de unión	Identificador exclusivo
ID de construcción	Identifica la construcción en la que se hace referencia a la unión.
SQL de unión	Tablas de unión
SQL Where	Cláusula Where (condiciones de unión)
Indicación de fecha y hora	Fecha y hora en que se creó la entidad Unión.

Entidad Comentarios locales

Esta entidad describe un comentario local. Sólo está disponible en el dominio de Comentarios, que está restringido a los usuarios administradores. Esta entidad sólo incluye comentarios locales, para procesos y conjuntos de resultados que se ejecutan localmente. Los comentarios que se pueden compartir se definen en la entidad Comentarios.

Tabla 59. Entidad Comentarios locales

Atributo	Descripción
Creador de comentario	Usuario de Guardium que creó el comentario.
Referencia de comentario	Indica el elemento al que se adjunta el comentario - una consulta, un resultado del proceso de auditoría u otro comentario, por ejemplo.
Contenido de comentario	El texto completo del comentario.
Indicación de fecha y hora	Fecha y hora en que se creó el comentario.
Año de indicación de fecha y hora	Solo año desde la indicación de fecha y hora
Día de semana de indicación de fecha y hora	Solo día de la semana desde la indicación de fecha y hora.
Hora de indicación de fecha y hora	Solo hora desde la indicación de fecha y hora.
Fecha de indicación de fecha y hora	Solo fecha desde la indicación de fecha y hora.
Descripción de objeto	Nombre del objeto desde el que se ha definido el comentario. Por ejemplo, un comentario definido en una incidencia tiene una descripción de objeto INCIDENT.
Asociaciones de registro	Una lista de registros a los que está asociado este comentario local.

Vista de ubicación

Cómo determinar qué días no están archivados.

Utilice una consulta (separador Herramientas > Creación de informes > Creador de informes > consulta Vista de ubicación) que se puede modificar para crear un informe mostrando los archivos archivados. Este informe lista todos los archivos con fechas de archivado. Las fechas que no aparecen en este informe indican archivos que no se han archivado. Si es necesario, ejecute archivar para las fechas que no aparecen en la lista.

Tabla 60. Entidad Vista de ubicación

Atributo	Descripción
Desde fecha	Fecha de inicio
Hasta fecha	Fecha de finalización
Agregador	Sistema Guardium en el que se ha generado el archivo. Sin embargo, puede ser un recopilador, no tan sólo un agregador.
Host	Nombre de host
Nombre de usuario	Nombre de usuario
Vía de acceso	Vía de acceso a los archivos
Tipo de sistema	Tipo de protocolo utilizado al archivar. Puede ser SCP o FTP o Centera o TSM.
Recuento de destinos	Destinos de archivado

Entidad Correlación de inicio de sesión

Obsoleto desde la versión 4.0 de Guardium. Ésta era la única entidad del dominio Seguimiento de rastreo de acceso, que ha quedado obsoleto a partir de la versión 4.0 de S-TAP. Si tiene consultas o informes antiguos que utilizan ese dominio, no funcionarán en este release, y cualquier información de inicio de sesión de base de datos registrada en dicho dominio será anterior a la instalación de la versión 4.0 de S-TAP.

Entidad Texto del mensaje

Para una alerta de umbral, el texto del mensaje.

Tabla 61. Entidad Texto del mensaje

Atributo	Descripción
ID de texto de mensaje	Identifica de forma exclusiva el texto del mensaje
Asunto del mensaje	Asunto del mensaje (para un mensaje de correo electrónico, por ejemplo).
Texto del mensaje	Texto del mensaje.
Huso horario original	Desplazamiento de UTC. Esto se realiza en concreto para los agregadores que tienen recopiladores en distintos husos horarios y, por lo tanto, actividades que se han realizado en distintas horas no parecen como si se hubiesen producido a la misma hora al importarlas al agregador. Por ejemplo, en un agregador que agrega datos de husos horarios diferentes, puede ver el inicio de sesión de un registro a las 21:00 con un huso horario original UTC-02:00 y otro registro de inicio de sesión a las 21:00 en un huso horario original UTC-05:00. Esto significa que estos sucesos se produjeron con una diferencia de 3 horas, pero respectivamente en la misma hora (21:00 h).

Entidad Mensajes enviados

Para cada mensaje de alerta de umbral enviado, el tipo de mensaje, los destinatarios, el estado y la fecha de dicho mensaje.

Tabla 62. Entidad Mensajes enviados

Atributo	Descripción
ID de mensaje	Identifica el mensaje de forma exclusiva
Tipo de mensaje	Tipo de mensaje.
Enviado a	Uno o varios destinatarios del mensaje.
Estado de mensaje	Estado de mensaje: FALLO La operación ha fallado. ESPERA El mensaje todavía no se ha enviado. ENVIADO El mensaje se ha enviado.
Fecha de mensaje	Fecha de envío del mensaje.
Contexto de mensaje	Tipo de mensaje: INFORMACIÓN Mensaje informativo. AVISO Posible condición de error. ALERTA Alerta de umbral o tiempo real. ERROR Condición de error de software o hardware. DEPURACIÓN Mensaje de depuración.
Remitente del mensaje	Módulo que crea el mensaje; por ejemplo, monitor o GuardiumJetspeedUser.

Atributo	Descripción
Huso horario original	Desplazamiento de UTC. Esto se realiza en concreto para los agregadores que tienen recopiladores en distintos husos horarios y, por lo tanto, actividades que se han realizado en distintas horas no parecen como si se hubiesen producido a la misma hora al importarlas al agregador. Por ejemplo, en un agregador que agrega datos de husos horarios diferentes, puede ver el inicio de sesión de un registro a las 21:00 con un huso horario original UTC-02:00 y otro registro de inicio de sesión a las 21:00 en un huso horario original UTC-05:00. Esto significa que estos sucesos se produjeron con una diferencia de 3 horas, pero respectivamente en la misma hora (21:00 h).

Entidad Valores de supervisor

Una entidad Valores de supervisor se crea para cada inserción, actualización o supresión registrada, con detalles del cambio (nombre de tabla, acción, texto SQL, etc.).

Tabla 63. Entidad Valores de supervisor

Atributo	Descripción
Indicación de fecha y hora	Fecha y hora en que se registró el cambio en el dispositivo Guardium. Esta indicación de fecha y hora se crea durante la operación de subida de datos. No es en el momento en que se registró en la base de datos de auditoría. Para obtener ese instante, utilice la entidad Indicación de fecha y hora de auditoría.
Fecha de indicación de fecha y hora	Solo fecha desde la indicación de fecha y hora.
Hora de indicación de fecha y hora	Solo hora desde la indicación de fecha y hora.
Año de indicación de fecha y hora	Solo año desde la indicación de fecha y hora
Día de semana de indicación de fecha y hora	Solo día de la semana desde la indicación de fecha y hora.
IP de servidor	Dirección IP del servidor de bases de datos.
Tipo de BD	Tipo de base de datos.
Nombre de servicio	Sólo Oracle. Nombre del servicio de base de datos.
Nombre de base de datos	Solo DB2, Informix, Sybase, MS SQL Server. Nombre de base de datos.
Clave primaria de auditoría	Solo para Sybase y MS SQL Server. Clave primaria utilizada para relacionar los valores antiguos y nuevos (que se deben registrar de forma separada para estos tipos de base de datos).
Nombre de inicio de sesión de auditoría	Nombre de usuario de base de datos definido en el origen de datos.
Nombre de tabla de auditoría	Nombre de la tabla que ha cambiado.
Propietario de auditoría	Propietario de la tabla cambiada.
Acción de auditoría	Insertar, actualizar o suprimir.
Valor anterior de auditoría	Una lista separada por comas de valores anteriores, en el formato: nombre-columna=valor_columna,
Valor nuevo de auditoría	Una lista separada por comas de valores nuevos, en el formato: nombre-columna=valor_columna,
Texto SQL	Sólo disponible con Oracle 9. Sentencia SQL completa que origina el cambio del valor.
ID desencadenado	ID exclusivo (en esta base de datos de auditoría) generado para el cambio.
Indicación de fecha y hora de auditoría	Fecha y hora en que se ha ejecutado el desencadenante.
Fecha de indicación de fecha y hora de auditoría	Parte de la fecha de la indicación de fecha y hora.
Hora de indicación de fecha y hora de auditoría	Parte de la hora de la indicación de fecha y hora de auditoría.
Día de semana de indicación de fecha y hora de auditoría	Día de la semana de la indicación de fecha y hora de auditoría.
Año de indicación de fecha y hora de auditoría	Año de la indicación de fecha y hora de auditoría.
Huso horario original	Desplazamiento de UTC. Esto se realiza en concreto para los agregadores que tienen recopiladores en distintos husos horarios y, por lo tanto, actividades que se han realizado en distintas horas no parecen como si se hubiesen producido a la misma hora al importarlas al agregador. Por ejemplo, en un agregador que agrega datos de husos horarios diferentes, puede ver el inicio de sesión de un registro a las 21:00 con un huso horario original UTC-02:00 y otro registro de inicio de sesión a las 21:00 en un huso horario original UTC-05:00. Esto significa que estos sucesos se produjeron con una diferencia de 3 horas, pero respectivamente en la misma hora (21:00 h).

Entidad Cambios supervisados

Esta entidad se crea cada vez que cambia un elemento supervisado. Identifica el elemento supervisado en la instancia CAS y apunta a los datos guardados de la modificación.

Tabla 64. Entidad Cambios supervisados

Atributo	Descripción

Atributo	Descripción
Identificador de cambio	Identificador exclusivo del cambio
Tiempo de muestreo	Indicación de fecha y hora (fecha y hora del host) en que se ha tomado la muestra
ID de configuración de auditoría	Identifica la configuración de host
ID de datos guardados	Identifica la entidad Datos guardados para este cambio
ID de etiqueta de estado de auditoría	Identifica la entidad de Configuración de host para este cambio
Indicación de fecha y hora	Fecha y hora en que se creó este registro en el servidor (reloj de servidor de dispositivo Guardium)
MD5	Indica si la comparación se realiza o no calculando una suma de comprobación utilizando el algoritmo MD5 y comparando dicho valor con el valor calculado la última vez que se comprobó el elemento. El valor predeterminado es no utilizar MD5. Si se utiliza MD5 pero el tamaño de los datos a tratar es mayor que el Límite de tamaño de MD5 configurado para el host CAS, se omitirá el cálculo y la comparación MD5. Independientemente de si se utiliza o no MD5, tanto el valor actual de la indicación de fecha y hora de la última modificación para el elemento y el tamaño del elemento se comparan con los valores que se han guardado la última vez que se comprobó el elemento.
Propietario	Solo en Unix. Si el tipo de elemento es un archivo, el propietario del archivo.
Permisos	Solo en Unix. Si el tipo de elemento es un archivo, los permisos del archivo.
Tamaño	El tamaño de archivo, con los siguientes valores especiales: -1 = El archivo existe, pero tiene cero bytes 0 (cero) = El archivo no existe, pero este nombre de archivo se está supervisando (nunca ha existido o puede ser que se haya suprimido)
Última modificación	Indicación de fecha y hora de la última modificación, tomada del sistema de archivos en el tiempo del muestreo
Fecha de última modificación	Fecha de la última modificación
Hora de última modificación	Hora de la última modificación
Día de la semana de la última modificación	Día de la semana de la última modificación
Año de última modificación	Año de la última modificación
Grupo	Solo en Unix. Si el tipo de elemento es un archivo, el propietario del grupo.

Entidad Detalles del elemento supervisado

La entidad Detalles de elemento supervisado se crea para cada elemento supervisado en una instancia CAS.

Tabla 65. Entidad Detalles del elemento supervisado

Atributo	Descripción
ID de configuración de auditoría	Identifica la configuración de host
Indicación de fecha y hora	Indicación de fecha y hora para la creación de la entidad
ID de plantilla	Identifica la plantilla de elementos de este elemento supervisado
Elemento supervisado	Dependiendo del tipo de auditoría, es el script SQL o SO, el entorno, la variable de registro o el nombre de archivo. Por lo que respecta al patrón de archivo definido en una plantilla de elemento, habrá una entidad de detalle de elemento supervisado independiente para cada archivo que coincida con el patrón. No habrá una entidad de detalle de elemento supervisado para el propio patrón de archivo. Si se utiliza un patrón de archivo, siempre estará disponible en el atributo de Contenido de plantilla.
ID de conjunto de configuración de auditoría	Identifica el conjunto de plantillas en la configuración de host
Tipo de auditoría	Tipo de elemento supervisado: Script de SO o Script SQL: El texto real o la vía de acceso a un script de sistema operativo o SQL, cuya salida se comparará con la salida producida la próxima vez que se ejecute Variable de entorno o variable de registro: Una variable de entorno o una variable de registro (Windows) Archivo: Un patrón o un archivo específico para identificar un conjunto de archivos
Habilitado	Indica si la plantilla está habilitada o no
En sincronización	Indica si la definición del elemento de plantilla en el servidor coincide con la definición de elemento de plantilla en el host de CAS
Frecuencia de auditoría	Intervalo máximo en el que se va a probar el elemento
Utilizar MD5	Indica si la comparación se realiza o no calculando una suma de comprobación utilizando el algoritmo MD5 y comparando dicho valor con el valor calculado la última vez que se comprobó el elemento. El valor predeterminado es no utilizar MD5. Si se utiliza MD5 pero el tamaño de los datos a tratar es mayor que el Límite de tamaño de MD5 configurado para el host CAS, se omitirá el cálculo y la comparación MD5. Independientemente de si se utiliza o no MD5, tanto el valor actual de la indicación de fecha y hora de la última modificación para el elemento y el tamaño del elemento se comparan con los valores que se han guardado la última vez que se comprobó el elemento.
Guardar datos	Cuando se marca, la versión anterior del elemento se puede comparar con la versión actual
Descripción	Descripción opcional de la instancia

Atributo	Descripción
Contenido de plantilla	Entrada de plantilla que es la base para este elemento supervisado, establecido desde el atributo Nombre de acceso de la entidad Plantilla cuando se creó la instancia. Normalmente será el mismo que el elemento supervisado, pero en el caso de que se haya utilizado un patrón de archivo en la plantilla, éste será el patrón de archivo.

Entidad Objeto

Se crea una instancia de esta entidad para cada objeto en un esquema exclusivo.

Tabla 66. Entidad Objeto

Atributo	Descripción
ID de objeto	Identifica el objeto de forma exclusiva.
ID de construcción	Identifica de forma exclusiva la construcción en la que se hace referencia al objeto.
Esquema	Esquema de base de datos para el objeto. Nota: Este atributo está en desuso puesto que nunca se cumplimenta.
Nombre de objeto	Nombre del objeto.
Módulo1 de objeto de aplicación	Identifica de forma exclusiva el módulo de objeto de aplicación.

ID de objeto e ID de construcción sólo están disponibles a los usuarios con el rol de administrador.

Entidad Mandato de objeto

Describe una entidad de mandato de objeto.

Tabla 67. Entidad Mandato de objeto

Atributo	Descripción
Objeto/Mandato	Valor de objeto combinado con un valor de mandato.

Entidad Campo de objeto

Describe una entidad de campo de objeto. Los campos de nota sin objetos no se mostrarán en los informes que incluyen el objeto.

Tabla 68. Entidad Campo de objeto

Atributo	Descripción
Objeto/Campo	Valor de objeto combinado con un valor de campo.

Entidad Infracción de reglas de política

Esta entidad se crea cada vez que se registra una infracción de regla de política. No todas las infracciones de reglas de política se registran, consulte la descripción de las acciones de regla en el Capítulo 11: Creación de políticas. La regla de acceso que origina la infracción estará disponible en la Entidad Regla de acceso dependiente (descrita anteriormente).

Tabla 69. Entidad Infracción de reglas de política

Atributo	Descripción
ID de registro de infracción	Identifica de forma exclusiva la entidad de la infracción.
Nombre de usuario de aplicación	Nombre del usuario que origina la infracción de la regla de política.
Serie SQL completo	Serie SQL que origina la infracción de la regla de política.
Indicación de fecha y hora	Se crea cuando se registra la infracción de regla de política. No todas las infracciones de reglas de política se registran, consulte la descripción de las acciones de regla en el Capítulo 11: Creación de políticas.
Fecha de indicación de fecha y hora	Solo fecha desde la indicación de fecha y hora.
Hora de indicación de fecha y hora	Solo hora desde la indicación de fecha y hora.
Día de semana de indicación de fecha y hora	Solo día de la semana desde la indicación de fecha y hora.
Año de indicación de fecha y hora	Solo año desde la indicación de fecha y hora
Mensaje enviado	Texto del mensaje de infracción de regla de política que envió.
Total de apariciones	Recuento de apariciones que desencadenaron la infracción.
ID de suceso de aplicación	ID de suceso de aplicación (si hay, se establece utilizando la API de sucesos de aplicación)
Descripción de regla de acceso	Descripción de la regla desde su definición.
Nombre de categoría	Categoría definida para la regla.
Gravedad	Gravedad definida para la regla (la gravedad de una incidencia a la que se asigna puede ser diferente).
Número de incidencia	Si se ha asignado a una incidencia, es el número de incidencia.

Atributo	Descripción
Nombre de clasificación	Nombre de proceso de clasificación.
ID de construcción	Identifica de forma exclusiva la construcción en la que se ha referenciado.
ID de ejecución de proceso CLS	ID de ejecución del trabajo del proceso de clasificación.
Huso horario original	Desplazamiento de UTC. Esto se realiza en concreto para los agregadores que tienen recopiladores en distintos husos horarios y, por lo tanto, actividades que se han realizado en distintas horas no parecen como si se hubiesen producido a la misma hora al importarlas al agregador. Por ejemplo, en un agregador que agrega datos de husos horarios diferentes, puede ver el inicio de sesión de un registro a las 21:00 con un huso horario original UTC-02:00 y otro registro de inicio de sesión a las 21:00 en un huso horario original UTC-05:00. Esto significa que estos sucesos se produjeron con una diferencia de 3 horas, pero respectivamente en la misma hora (21:00 h).

El ID de registro de infracción sólo está disponible para los usuarios que tienen el rol de administrador.

Entidad Objeto calificado

Una *tupla* combina varios atributos de forma conjunta para formar un miembro de grupo individual. En este caso, los campos IP de servidor, nombre de servicio, nombre de BD, usuario de BD y objeto se combinan de forma conjunta.

Tabla 70. Entidad Objeto calificado

Atributo	Descripción
Objeto calificado	Tupla - IP de servidor, nombre de servicio, nombre de BD, usuario de BD, objeto

Entidad Conexiones inesperadas

Se crea una instancia para cada conexión de base de datos que el proceso Hunter de S-TAP detecte, pero no las del propio S-TAP, indicando que la conexión ha omitido las vías de acceso supervisadas por S-TAP.

Tabla 71. Entidad Conexiones inesperadas

Atributo	Descripción
Indicación de fecha y hora	Valor de indicación de fecha y hora creado cuando el dispositivo Guardium registra la conexión inesperada de la que Hunter informa.
Nombre de host del servidor	Nombre de host del servidor de bases de datos.
Programa fuente	Nombre de programa fuente para la conexión.
Puerto de origen	Puerto de origen para la conexión.
PID de origen	ID de proceso de origen.
Programa de destino	Nombre del programa de destino para la conexión.
Puerto de destino	Puerto de destino para la conexión.
PID de destino	ID de proceso de destino.
Usuario de SO	Nombre de cuenta de usuario de sistema operativo.
Tipo de IPC	Tipo de comunicaciones entre procesos (IPC) utilizadas para la conexión, que puede ser uno de los siguientes: Memoria compartida SHM IPv4 Internet Protocol versión 4 IPv5 Internet Protocol versión 6 Conducto con nombre FIFO Conducto PIPE Simple INET Internet Protocol (HPUX)
Tipo de servidor de BD	Tipo de servidor de base de datos: Oracle, DB2, Informix o Sybase.
Huso horario original	Desplazamiento de UTC. Esto se realiza en concreto para los agregadores que tienen recopiladores en distintos husos horarios y, por lo tanto, actividades que se han realizado en distintas horas no parecen como si se hubiesen producido a la misma hora al importarlas al agregador. Por ejemplo, en un agregador que agrega datos de husos horarios diferentes, puede ver el inicio de sesión de un registro a las 21:00 con un huso horario original UTC-02:00 y otro registro de inicio de sesión a las 21:00 en un huso horario original UTC-05:00. Esto significa que estos sucesos se produjeron con una diferencia de 3 horas, pero respectivamente en la misma hora (21:00 h).

Entidad Regla

Se puede utilizar para la entidad Regla de política instalada o la entidad Regla de política de acceso. Hay una para cada una de las políticas instaladas o las políticas de acceso. Además de los campos de ID (que identifican de forma exclusiva los componentes en la base de datos interna), todos estos campos se describen en el tema de ayuda de Políticas.

- GDM_INSTALLED_POLICY_RULES_ID - Identifica una regla de política instalada.
- ACCESS_RULE_ID - Identifica una regla de acceso.
- Descripción de regla - Desde la definición de política.

- Posición de regla - Posición dentro de la política.
- Tipo de regla - Acceso, Excepción o Extrusión.
- LAST_ACCESSED - Última
- IP de cliente - Desde la definición de regla.
- Máscara de red de cliente - Desde la definición de regla.
- Grupo de IP de cliente - Desde la definición de regla.
- IP de servidor - Desde la definición de regla.
- Máscara de IP de servidor - Desde la definición de regla.
- Cliente MAC - Desde la definición de regla.
- Protocolo de red - Desde la definición de regla.
- Grupo de protocolos de red - Desde la definición de regla.
- Campo - Desde la definición de regla.
- Grupo de campos - Desde la definición de regla.
- Objeto - Desde la definición de regla.
- Grupo de objetos - Desde la definición de regla.
- Mandato - Desde la definición de regla.
- Grupo de mandatos - Desde la definición de regla.
- Grupo de objetos-campos - Desde la definición de regla.
- Tipo de BD - Desde la definición de regla.
- Nombre de servicio - Desde la definición de regla.
- Grupo de nombres de servicio - Desde la definición de regla.
- Nombre de BD - Desde la definición de regla.
- Grupo de nombres de BD - Desde la definición de regla.
- Usuario de BD - Desde la definición de regla.
- Grupo de usuarios de BD - Desde la definición de regla.
- Usuario de aplicación - Desde la definición de regla.
- Grupo de usuarios de Aplicación - Desde la definición de regla.
- Usuario de SO - Desde la definición de regla.
- Grupo de usuarios de SO - Desde la definición de regla.
- Aplic. origen - Desde la definición de regla.
- Grupo de programas de origen - Desde la definición de regla.
- Patrón/Patrón XML - Desde la definición de regla.
- Periodo - Desde la definición de regla.
- Recuento mínimo - Desde la definición de regla.
- Intervalo de restablecimiento - Desde la definición de regla.
- Continuar en la siguiente regla / Revocar - Desde la definición de regla.
- Val. Grab. - Desde la definición de regla.
- Existe suceso de aplicación - Desde la definición de regla.
- Tipo de suceso - Desde la definición de regla.
- Valor de texto de suceso de aplicación - Desde la definición de regla.
- Valor de fecha de suceso de aplicación - Desde la definición de regla.
- Nombre de usuario de suceso - Desde la definición de regla.
- Código de error - Desde la definición de regla.
- Tipo de excepción - Desde la definición de regla.
- Nombre de categoría - Desde la definición de regla.
- Nombre de clasificación - Desde la definición de regla.
- Gravedad - Desde la definición de regla.
- Patrón de datos - Desde la definición de regla.
- Patrón de SQL - Desde la definición de regla.
- Patrón de máscara - Desde la definición de regla.
- IP cliente / Grupo - Proporciona la posibilidad de visualizar un único atributo y sus relacionados (si los hay) en una columna individual del informe.
- IP servidor / Grupo - Proporciona la posibilidad de visualizar un único atributo y sus relacionados (si los hay) en una columna individual del informe.
- Protocolo de red / Grupo - Proporciona la posibilidad de visualizar un único atributo y sus relacionados (si los hay) en una columna individual del informe.
- Nombre de campo / Grupo - Proporciona la posibilidad de visualizar un único atributo y sus relacionados (si los hay) en una columna individual del informe.
- Nombre de objeto / Grupo - Proporciona la posibilidad de visualizar un único atributo y sus relacionados (si los) en una columna individual del informe.
- Mandato / Grupo - Proporciona la posibilidad de visualizar un único atributo y sus relacionados (si los hay) en una columna individual del informe.
- Nombre de servicio / Grupo - Proporciona la posibilidad de visualizar un único atributo y sus relacionados (si los hay) en una columna individual del informe.
- Nombre de BD / Grupo - Proporciona la posibilidad de visualizar un único atributo y sus relacionados (si los hay) en una columna individual del informe.
- Usuario de aplicación / Grupo - Proporciona la posibilidad de visualizar un único atributo y sus relacionados (si los hay) en una columna individual del informe.
- Usuario de SO / Grupo - Proporciona la posibilidad de visualizar un único atributo y sus relacionados (si los hay) en una columna individual del informe.
- Programa fuente / Grupo - Proporciona la posibilidad de visualizar un único atributo y sus relacionados (si los hay) en una columna individual del informe.
- Código de error / Grupo - Proporciona la posibilidad de visualizar un único atributo y sus relacionados (si los hay) en una columna individual del informe.
- Texto / Numérico / Fecha de suceso de aplicación - Los atributos de fecha, numérico y texto de sucesos de aplicación.
- Categoría / Clasificación - La categoría y clasificación combinadas para la regla.
- GDM_Installed_Policy_Header_ID - Identifica una cabecera de política instalada.

Nota: GDM_INSTALLED_POLICY_RULES_ID y ACCESS_RULE_ID sólo están disponibles a los usuarios con el rol de administrador.

Entidad Regla de acción

Se puede utilizar para entidad de acción de regla de Política instalada o la entidad de acción de regla de Política de acceso. Hay una para cada una de las políticas instaladas o las políticas de acceso.

- Secuencia - Secuencia de la acción dentro de la regla.
- Acción
  - Bloquear la solicitud - Consulte Acciones de bloqueo en Políticas.
  - Registrar o ignorar la infracción en traffik - Consulte Registrar o ignorar acciones en Política.
  - Alerta - Consulte Acciones de alerta en Políticas.

Entidad Datos guardados

Se crea una entidad Datos guardados cada vez que se detecte un cambio para un elemento que se está supervisando, si el recuadro Mantener datos está marcado para ese elemento en la definición de plantilla de elemento.

Tabla 72. Entidad Datos guardados

Atributo	Descripción
ID de datos guardados	Identifica de forma exclusiva el elemento de datos guardado
Datos guardados	Datos reales guardados
Indicación de fecha y hora	Indicación de fecha y hora del momento en que se registró la entidad de datos guardados en la base de datos del servidor
Identificador de cambio	Identifica la entidad de cambios supervisados para esta entidad de datos guardados

El ID de datos guardados solo está disponible a los usuarios con el rol de administrador.

Entidad IP servidor-Puerto servidor

Describe una entidad de IP servidor-puerto de servidor.

Tabla 73. Entidad IP servidor-Puerto servidor

Atributo	Descripción
IP servidor/Puerto servidor	Valor de IP de servidor combinado con un valor de puerto de servidor.

Entidad Sesión

Esta entidad se crea para cada sesión de base de datos de cliente/servidor.

Tabla 74. Entidad Sesión

Atributo	Descripción
ID global	Identifica de forma exclusiva el acceso de sesión.
ID de sesión	Identifica la sesión de forma exclusiva.
ID de acceso	Identifica de forma exclusiva el periodo de acceso.
Indicación de fecha y hora	Inicialmente, se crea una indicación de fecha y hora para la primera solicitud en una conexión cliente-servidor donde no hay una sesión activa en curso. Más adelante, se actualiza cuando se cierra la sesión, o cuando se marca como inactiva después de un periodo de tiempo ampliado sin actividad observada. Al realizar un seguimiento de la información de sesión, es probable que esté más interesado en los atributos Inicio de sesión y Fin de sesión que en el atributo Indicación de fecha y hora.
Fecha de indicación de fecha y hora	Solo fecha desde la indicación de fecha y hora.
Hora de indicación de fecha y hora	Solo hora desde la indicación de fecha y hora.
Día de semana de indicación de fecha y hora	Solo día de la semana desde la indicación de fecha y hora.
Año de indicación de fecha y hora	Solo año desde la indicación de fecha y hora
Inicio de sesión	Fecha y hora en que se inició la sesión. Inicio de sesión es también una entidad principal. Acceda a esta entidad secundaria pulsando en la entidad primaria Sesión.
Fecha de inicio de sesión	Solo fecha desde el inicio de sesión.
Hora de inicio de sesión	Solo hora desde el inicio de sesión.
Día de semana de inicio de sesión	Solo día de semana desde el inicio de sesión.
Año de inicio de sesión	Solo año desde el inicio de sesión.
Puerto de cliente	Número de puerto del cliente.
Puerto de servidor	Número de puerto de servidor.
Distintivo inactivo	Predeterminado 0 - Abrir para las sesiones generadas por el paquete SQL. 1 - Cerrado (desconectado/ recibido final de sesión). 2 - Probablemente cerrado; no cerrado sin paquetes durante un periodo considerable. 3 - Para sesiones generadas desde paquetes que no son de SQL.
TTL	Reservado para ser utilizado únicamente por el rol de administrador.
Fin de sesión	Fecha y hora en la que finalizó la sesión. Fin de sesión es también una entidad principal. Acceda a esta entidad secundaria pulsando en la entidad primaria Sesión.
Fecha de fin de sesión	Solo fecha desde el fin de sesión.
Hora de fin de sesión	Solo hora desde el fin de sesión.
Día semana de fin de sesión	Solo día de semana desde el fin de sesión.
Año de fin de sesión	Solo año desde el fin de sesión.

Atributo	Descripción
Nombre de base de datos	Nombre de la base de datos para la sesión (sólo para MSSQL o Sybase). Nota: Para Oracle, el Nombre de base de datos puede contener información adicional y específica de la aplicación como, por ejemplo, el módulo que se está ejecutando actualmente para una sesión que se ha establecido en la columna MODULE de la vista V$SESSION.
Sesión ignorada	Indica si alguna parte de la sesión se ha ignorado (empezando en algún punto en el tiempo).
Ignorado desde	Indicación de fecha y hora creada al empezar a ignorar esta sesión.
Cadena de UID	Para una sesión de informada por Unix S-TAP (solo modalidad K-Tap), muestra la cadena de usuarios de SO, cuando los usuarios hacen su con un nombre de usuario diferente. Los valores que aparecen aquí dependen de la plataforma del SO, por ejemplo, bajo AIX la serie IBM IBM IBM puede aparecer como un prefijo. Nota: para zonas de Solaris, se pueden notificar los ID de usuario en lugar de los nombres de usuario en la Cadena de UID.
ID de sesión antigua	Apunta a la sesión a partir de la cual se ha creado esta sesión. Cero si es la primera sesión de la conexión.
ID de terminal	ID de terminal de la conexión, utilizado internamente para resolver la información de sesión.
ID de proceso	ID de proceso del cliente inició la conexión (no siempre está disponible).
Cadena de UID comprimida	Valores comprimidos. Véase Cadena de UID.
Duración (segs)	Indica el periodo de tiempo entre el inicio de sesión y el fin de sesión (en segundos).
Huso horario original	Desplazamiento de UTC. Esto se realiza en concreto para los agregadores que tienen recopiladores en distintos husos horarios y, por lo tanto, actividades que se han realizado en distintas horas no parecen como si se hubiesen producido a la misma hora al importarlas al agregador. Por ejemplo, en un agregador que agrega datos de husos horarios diferentes, puede ver el inicio de sesión de un registro a las 21:00 con un huso horario original UTC-02:00 y otro registro de inicio de sesión a las 21:00 en un huso horario original UTC-05:00. Esto significa que estos sucesos se produjeron con una diferencia de 3 horas, pero respectivamente en la misma hora (21:00 h).

ID global, ID de sesión e ID de acceso solo están disponibles a los usuarios con el rol de administrador.

Entidad Gravedad

La gravedad de la incidencia de una incidencia o infracción de política

Tabla 75. Entidad Gravedad

Atributo	Descripción
Descripción de gravedad	El código de gravedad será uno de los siguientes: INFORMACIÓN, BAJA, MEDIA, ALTA

Entidad Uso de almacenamiento intermedio de sniffer

El sistema crea esta entidad en el intervalo establecido por el mandato de CLI netfilter-buffer-size del sistema almacenamiento (cada 60 segundos de forma predeterminada).

Tabla 76. Entidad Uso de almacenamiento intermedio de sniffer

Atributo	Descripción
Indicación de fecha y hora	Hora en la que se creó el registro.
% CPU sniffer	Porcentaje de CPU utilizado por el sniffer.
% Mem sniffer	Porcentaje de memoria utilizada por el sniffer.
% CPU Mysql	Porcentaje de CPU utilizado por MySQL.
% Mem Mysql	Porcentaje de memoria utilizada por MySQL.
ID de proceso de sniffer.	Identificador de proceso de sniffer.
Mem sniffer	Cantidad de memoria utilizada por el sniffer.
Tiempo sniffer	Tiempo transcurrido utilizado por el sniffer.
Espacio de almacenamiento intermedio libre	Cantidad de espacio de almacenamiento intermedio libre.
Velocidad analizador	Velocidad a la que se analizan los mensajes.
Velocidad registrador	Velocidad a la que se registran los mensajes.
Longitud de cola de analizador	Tamaño de la cola de análisis.
Total analizador	Número total de mensajes analizados.
Longitud de cola de registrador	Tamaño de la cola del registrador.
Total de registrador	Número total de mensajes registrados.
Longitud de cola de sesión	Tamaño de la cola de sesión.
Total sesión	Número total de sesiones.
Datos de manejador	Datos de motor de procesos de sniffer internos.
Información adicional	Datos de motor de procesos de sniffer internos.

Atributo	Descripción
Paquetes perdidos de analizador	Paquetes perdidos por el analizador.
Eth0 recibido	Mensajes recibidos en ETH 0.
Eth0 enviado	Mensajes enviados en ETH 0.
Bases de datos supervisadas de registrador	Lista de tipos de base de datos que se están supervisando actualmente.
Paquetes de registrador ignorados por regla	Paquetes ignorados por la acción de la regla de política.
Recuento de sesiones de registrador	Recuento de sesiones registradas.
Uso de disco de Mysql	Uso de disco de MySQL.
Mysql activo	Indicador booleano de reinicio de base de datos interna (1=se reinició, 0=no se reinició).
Recibidos modalidad promiscua	Ratio de paquetes recibidos a través de las tarjetas de red para sniffer (puertos que no son de interfaz).
Conexiones finalizadas de sniffer	Número total de conexiones que se supervisaron y finalizaron desde que se reinició el motor de inspección.
Conexiones utilizadas de sniffer	Número total de conexiones que se están supervisando actualmente desde que se reinició el motor de inspección.
Paquetes de sniffer descartados	Paquetes descartados por el sniffer.
Paquetes ignorados de sniffer	Paquetes ignorados por el empleado.
Paquetes de sniffer regulados	Número total de conexiones que se han ignorado debido a la regulación desde que se reinició el motor de inspección.
Carga de CPU del sistema	Utilización de CPU del sistema.
Uso de memoria de sistema	Utilización de memoria del sistema.
Uso de disco raíz de sistema	Utilización de disco raíz del sistema.
Tiempo de actividad de sistema	Tiempo desde el último arranque.
Uso del disco Var del sistema	Utilización de disco var del sistema.
Sesiones normales	Recuento de sesiones normales.
Sesiones no abiertas	Recuento de sesiones no abiertas por el sniffer.
Tiempo de espera de sesión	Número de sesiones que han excedido el tiempo de espera.
Sesiones ignoradas	Recuento de sesiones ignoradas por el sniffer.
Sesiones cerradas directamente	Recuento de sesiones cerradas directamente.
Sesiones adivinadas	Recuento de sesiones adivinadas.
FD abiertos	Descriptores de archivo abiertos.
FD abiertos de BD	Descriptores de archivo abiertos de base de datos
Velocidad Di	
Longitud de cola Di	
Total Di	
Paquetes perdidos Di	
Solicitudes Flat Log	Solicitudes de Flat Log.

Definición de asesoramiento basado en SQL

Esta entidad describe una definición de asesoramiento basado en SQL

Tabla 77. Definición de asesoramiento basado en SQL

Atributo	Descripción
Vincular variable de salida	Opcional. Determina si el texto especificado en la sentencia SQL es un bloque de código de procedimiento que devolverá un valor se debe vincular a una variable interna de Guardium que se utilizará en la comparación para Comparar con valor.
Comparar con valor	Valor de comparación que se utilizará para compararlo con el valor de retorno de la sentencia SQL utilizando el operador de comparación.
Referencia externa	Referencia a CIS (Center for Internet Security) o CVE (Common Vulnerabilities and Exposures).
Operador	Operador que se utilizará para la condición.
Texto de recomendación para fallar	El texto recomendado cuando falle la prueba.

Atributo	Descripción
Texto de recomendación para pasar	El texto recomendado para cuando se pase la prueba.
Texto de resultado para fallar	El texto de resultado cuando falle la prueba.
Texto de resultado para pasar	El texto de resultado para cuando se pase la prueba.
Tipo de retorno	El tipo de retorno que se devolverá desde la sentencia SQL.
Descripción breve	Descripción breve de la prueba de asesoramiento.
SQL para detalles	Sentencia SQL para detalles, sentencia SQL que recupera una lista de series para generar una serie detallada de prefijo de detalle + lista de series.
SQL	Sentencia SQL que se ejecutará para la prueba.

Entidad SQL

Entidad SQL

Esta entidad se crea para cada serie exclusiva de SQL. Los valores se sustituyen por signos de interrogación - sólo se almacena el formato de la serie.

Tabla 78. Entidad SQL

Atributo	Descripción
SQL	Serie SQL.
ID de construcción	Identifica de forma exclusiva la construcción en la que el SQL aparece.
Información de vinculación	Información de vinculación para esta serie SQL.
SQL truncado	Indica si el SQL se ha truncado o no, donde: 0 - falso/no, no truncado 1 - verdadero/sí, truncado

Entidad Receptor de tareas

Indica la acción que el receptor de resultados necesita.

Tabla 79. Entidad Receptor de tareas

Atributo	Descripción
Acción necesaria	Indica si es necesario firmar la acción.

Entidad Resultados de tareas de listas de tareas pendientes

Indica el estado actual de los resultados.

Tabla 80. Entidad Resultados de tareas de listas de tareas pendientes

Atributo	Descripción
Estado	Indica el estado actual de los resultados.
(Esca) Acción necesaria	Indica si la acción de lista de tareas pendientes es necesaria.
Acción necesaria	Indica si es necesario firmar la acción.

Entidad Plantilla

Se crea una entidad Plantilla de CAS para cada plantilla de elemento dentro de un conjunto de plantillas. Un elemento es un patrón de archivo o archivo específico, un entorno o una variable de registro, la salida de un script SQL o sistema operativo, o la lista de usuarios conectados.

Tabla 81. Entidad Plantilla

Atributo	Descripción
ID de plantilla	Identificador exclusivo para la plantilla de elemento dentro del conjunto de todas las plantillas de elemento
ID de conjunto de plantillas	Identificador exclusivo para el conjunto de plantillas
Nombre de acceso	En función del tipo de auditoría, se trata del SO o del script SQL, entorno o valor de registro, o un nombre de archivo o un patrón de nombre de archivo
Tipo de auditoría	El tipo de elemento supervisado
Frecuencia de auditoría (minutos)	El intervalo máximo (en minutos) entre pruebas
Utilizar MD5	Indica si la comparación se realiza o no calculando una suma de comprobación utilizando el algoritmo MD5 y comparando dicho valor con el valor calculado la última vez que se comprobó el elemento. El valor predeterminado es no utilizar MD5. Si se utiliza MD5 pero el tamaño de los datos a tratar es mayor que el Límite de tamaño de MD5 configurado para el host CAS, se omitirá el cálculo y la comparación MD5. Independientemente de si se utiliza o no MD5, tanto el valor actual de la indicación de fecha y hora de la última modificación para el elemento y el tamaño del elemento se comparan con los valores que se han guardado la última vez que se comprobó el elemento.

Atributo	Descripción
Guardar datos	Indica si se ha marcado el recuadro de selección Mantener datos. Si es así, las versiones anteriores del elemento pueden compararse con la versión actual.
Editable	Indica si se puede modificar o no la plantilla. Las plantillas predeterminadas de Guardium no se pueden modificar. Además, una vez se ha utilizado un conjunto de plantillas en una instancia de CAS, no se puede modificar. En cualquier caso, un conjunto de plantillas siempre se puede clonar y el conjunto clonado se puede modificar.
Descripción	Descripción opcional de la plantilla
Indicación de fecha y hora	Fecha y hora de la última actualización de esta plantilla

El ID de plantilla y el ID de conjunto de plantillas sólo están disponibles a los usuarios con el rol de administrador.

Entidad Conjunto de plantillas

Se crea una entidad Conjunto de plantillas CAS para cada conjunto de plantillas, que es un conjunto de elementos de plantilla de un sistema operativo o una base de datos determinados.

Tabla 82. Entidad Conjunto de plantillas

Atributo	Descripción
ID de conjunto de plantillas	Un identificador exclusivo para el conjunto de plantillas, numerado secuencialmente
Tipo de SO	Sistema operativo: Unix o Windows
Tipo de BD	Tipo de base de datos: Oracle, MS-SQL, DB2, Sybase, Informix o N/D para una plantilla de sistema operativo.
Nombre de conjunto de plantillas	El nombre de la plantilla
Predeterminado	Indica si la plantilla es o no la predeterminada para la combinación de tipo de SO especificado y el tipo de BD
Editable	Indica si se puede modificar o no la plantilla. Las plantillas predeterminadas de Guardium no se pueden modificar. Además, una vez se ha utilizado un conjunto de plantillas en una instancia de CAS, no se puede modificar. En cualquier caso, un conjunto de plantillas siempre se puede clonar y el conjunto clonado se puede modificar.
Indicación de fecha y hora	Fecha y hora en que se actualizó la plantilla

El ID conjunto de plantillas solo está disponible a los usuarios con el rol de administrador.

Entidad Resultado de la prueba

Esta entidad se crea para cada conjunto de resultados de prueba.

Tabla 83. Entidad Resultado de la prueba

Atributo	Descripción
ID de resultado de prueba	Identifica el resultado de la prueba.
ID de resultado de asesoramiento	Identifica el conjunto de resultados del asesoramiento.
ID1 de prueba	Identifica la prueba.
ID de prueba de asesoramiento	Identifica la prueba de asesoramiento (tarea).
Puntuación de prueba	Puntuación de prueba devuelta.
ID de resultado de informe	Identifica el resultado del informe.
Distintivo de parámetro modificado	Indica si los parámetros se han modificado desde la última prueba.
Texto de resultado	Texto que ha devuelto la prueba.
Descripción de la prueba	Descripción desde la definición de prueba.
Recomendación	Recomendación que ha devuelto la prueba.
Descripción de puntuación	Descripción de la puntuación.
Serie de umbral	Solicitud de umbral para la prueba (por ejemplo, Número máximo de IP diferentes permitidas por usuario)
Gravedad	Gravedad asignada para el resultado de la prueba.
Categoría	Categoría para el resultado de la prueba.
ID1 de origen de datos de resultado de asesoramiento.	Identifica el origen de datos del resultado de la prueba.
Detalles de resultado	Detalles de la prueba.
Descripción de grupo de excepciones	Descripción del grupo de excepciones. Se cumplimenta cuando se ejecuta la prueba.

ID de resultado de prueba, ID de resultado de asesoramiento e ID de prueba de asesoramiento solo están disponibles a los usuarios con el rol de administrador.

Entidad Detalles de alerta de umbral

Esta entidad se crea cada vez que se desencadena una alerta de correlación.

Tabla 84. Entidad Detalles de alerta de umbral

Atributo	Descripción
ID de registro de alerta	Identifica de forma exclusiva la entidad de detalles de alerta.
Valor de consulta	Valor devuelto por la consulta.
Valor base	Valor asignado para la alerta estadística.
Desde fecha comprobada	La hora y fecha de inicio comprobada por la condición de alerta.
Hasta fecha comprobada	La hora y fecha de finalización comprobada por la condición de alerta.
Umbral de alerta	Umbral de alerta definido para la alerta.
Notificación enviada	Texto de la notificación enviada.
Indicación de fecha y hora	Creado sólo una vez, cuando se registra la alerta estadística.
Descripción de alerta	Descripción contenida en la definición de alerta.

El ID de registro de alertas sólo está disponible a los usuarios con el rol de administración.

Nivel de utilización de unidad

De forma predeterminada se proporcionan varios informes de utilización de unidad de forma predeterminada en Gestionar > Informes > Utilización de unidad, incluidos:

- Utilización de unidad: Muestra el nivel máximo de utilización de unidad de cada unidad en el marco temporal dado. Hay un desglose que muestra detalles para una unidad en todos los periodos dentro del marco temporal del informe.
- Distribución de la utilización de la unidad: Por unidad, este informe visualiza el porcentaje de periodos en el marco temporal del informe con niveles de utilización bajo, medio y alto.
- Umbrales de utilización: Se trata de un informe predefinido que visualiza los valores de umbral altos y bajos de todos los parámetros de utilización de unidad.
- Resumen diario de utilización de la unidad: Proporciona un resumen diario de los datos de utilización de unidad.

Además, el seguimiento de niveles de utilización de unidades permite a los usuarios crear informes y consultas personalizados.
Consejo: Habilite alias para todos los informes predefinidos utilizando los datos de utilización de la unidad para garantizar que los niveles de utilización de unidad se visualicen como series con significado en lugar de números. Por ejemplo, bajo, medio y alto en lugar de 1, 2 o 3.
La lista de atributos incluye:

- Nombre de host
- Inicio de periodo
- Número de reinicios
- Nivel de número de reinicios
- Memoria del sniffer
- Nivel de memoria de sniffer
- Memoria porcentual de MySQL
- Nivel de memoria porcentual de MySQL
- Espacio de almacenamiento intermedio libre
- Nivel de espacio de almacenamiento intermedio libre
- Cola de analizador
- Nivel de cola de analizador
- Cola de registrador
- Nivel de cola de registrador
- Uso de disco de MySQL
- Nivel de uso de disco de MySQL
- Carga de CPU del sistema
- Nivel de carga de CPU del sistema
- Uso del disco Var del sistema
- Nivel de uso del disco Var del sistema
- Nivel de utilización de unidad global
- Número de solicitudes
- Nivel de número de solicitudes
- Número de SQL completo
- Nivel de número de SQL completo
- Número de excepciones
- Nivel de número de excepciones
- Número de infracciones de política
- Nivel de número de infracciones de política
- Número de solicitudes de Flat Log
- Nivel de número de solicitudes de Flat Log

Nota: Cada parámetro tiene un valor y un nivel que se calcula en base al valor y a los umbrales.

Entidad Usuario

Identifica el usuario de Guardium definido como receptor de resultados de proceso de auditoría.

Tabla 85. Entidad Usuario

Atributo	Descripción
Nombre de inicio de sesión	Nombre de usuario de Guardium.
Nombre	Nombre del usuario de Guardium.
Apellido	Apellido del usuario de Guardium.

Atributo	Descripción
Dirección de correo electrónico	Dirección de correo electrónico definido por el usuario de Guardium.
Último activo	Indicación de fecha y hora de la última actividad de este usuario.

Tema principal: Dominios, entidades y atributos

Informes de titularidad de base de datos

Puede utilizar informes de titularidad de base de datos para verificar que los usuarios sólo tienen acceso a los datos adecuados. El sistema Guardium incluye informes predefinidos de titularidad de base de datos para varios tipos de bases de datos.

Nota: Los Informes de titularidades de BD son componentes opcionales habilitados por la clave de producto. Si estos componentes no se han habilitado, las opciones listadas a continuación no aparecerán en las selecciones de Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas.

Los informes de titularidad predefinidos se listan a continuación. Aparecen como nombres de dominio en las selecciones de Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas:

- Dominios de titularidades de BD de Oracle
- Dominios de titularidades de BD de MYSQL
- Dominios de titularidades de BD de DB2
- Dominios de titularidades de BD de DB2 for i 6.1 y 7.1
- Dominios de titularidades de BD de SYBASE
- Dominios de titularidades de BD de Informix
- Dominios de titularidades de BD de MSSQL 2000
- Dominios de titularidades de BD de MSSQL 2005
- Dominios de titularidades de BD de Netezza
- Dominios de titularidades de BD de Teradata DB
- Dominios de titularidades de BD de PostgreSQL

Consulte también Optimización de titularidades.

Titularidades de BD de Oracle

Se proporcionan los siguientes dominios para facilitar la carga y notificación de las Titularidades de BD de Oracle. Cada uno de los siguientes dominios tiene una sola entidad (con el mismo nombre), y hay un informe predefinido para cada dominio. Todos estos dominios están disponibles en las selecciones Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas. Al igual que con otras entidades e informes predefinidos, éstos no se pueden modificar, pero puede clonar y, a continuación, personalizar sus propias versiones de cualquiera de estos informes o dominios. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador Titularidades de BD.

Oracle

- ORA: Cuentas de ALTER SYSTEM - Cuentas con privilegios ALTER SYSTEM y ALTER SESSION
- ORA: Cuentas con BECOME USER - Cuentas con privilegios BECOME USER
- Todas las opc. de priv. y de admin. del sist. de ORA - Informe que muestra todos los privilegios del sistema y la opción admin para usuarios y roles
- Priv. de obj. y columnas de ORA - Privilegios de objetos y columnas otorgados (con o sin opción de otorgar)
- Acceso a objetos ORA mediante PUBLIC - Acceso a objetos mediante PUBLIC
- Privilegios de objetos ORA - Privilegios de objetos mediante la cuenta de base de datos no en el rol SYS y no en el rol DBA
- Ej. priv. de ORA PUBLIC en proc. SYS - Privilegio de ejecución en procedimientos SYS PL/SQL asignados a PUBL
- Roles otorgados de ORA - Roles otorgados a usuarios y roles
- Priv. de sis. de ORA otorgado - Informe jerárquico que muestra el privilegio de sistema otorgado a los usuarios que incluye las definiciones recursivas (es decir, privilegios asignados a los roles y, a continuación, estos roles asignados a los usuarios)
- ORA: Cuentas SYSDBA y SYSOPER - Cuentas con los privilegios SYSDBA y SYSOPER

Para que las titularidades puedan subir datos desde varios orígenes de datos, el requisito general es que el inicio de sesión, que se utiliza para acceder a la base de datos, pueda leer las tablas utilizadas en la consulta (que está oculta para todas las titularidades).

La siguiente lista (con cabecera de línea de comentarios) detalla los privilegios mínimos necesarios, en la tabla de base de datos (o vista de la tabla de base de datos), para que la titularidad funcione.

```
/* Es necesario seleccionar un privilegio para estas tablas/vistas */

grant select on sys.dba_tab_privs to sqlguard;

grant select on sys.dba_roles to sqlguard;

grant select on sys.dba_users to sqlguard;

grant select on sys.dba_role_privs to sqlguard;

grant select on sys.dba_sys_privs to sqlguard;

grant select on sys.obj$ to sqlguard;

grant select on sys.user$ to sqlguard;

grant select on sys.objauth$ to sqlguard;

grant select on sys.table_privilege_map to sqlguard;

grant select on sys.dba_objects to sqlguard;

grant select on sys.v_$pwfile_users to sqlguard;
```

grant select on sys.dba_col_privs to sqlguard;

Titularidades de BD de MYSQL

Se proporcionan los siguientes dominios para facilitar la carga y la creación de informes sobre las Titularidades de BD de MYSQL. Cada uno de los siguientes dominios tiene una sola entidad (con el mismo nombre), y hay un informe predefinido para cada dominio. Todos estos dominios están disponibles en las selecciones Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas. Al igual que con otras entidades e informes predefinidos, éstos no se pueden modificar, pero puede clonar y, a continuación, personalizar sus propias versiones de cualquiera de estos informes o dominios. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador Titularidades de BD.

MYSQL: Las consultas que terminan por "_40" utilizan la versión más básica del esquema de mysql (para MySQL 4.0 y posterior). information_schema no ha cambiado desde que se introdujo en MySQL 5.0, por lo que hay un conjunto de _50 consultas, pero no hay _51 consultas. Las _50 consultas funcionan para MySQL 5.0 y 5.1 y para 6.0 cuando salga, ya que no se espera que information_schema cambie en 6.0. Las consultas que terminan por "_502" (MYSQL502) utilizan el nuevo information_schema, que contiene mucha más información y es mucho más parecido a un diccionario de datos verdadero.

- Privilegios 40 de base de datos de MYSQL
- Privilegios 40 de usuario de MYSQL
- Privilegios 40 de host de MYSQL
- Privilegios 40 de tabla de MYSQL
- Privilegios 500 de base de datos de MYSQL
- Privilegios 500 de usuario de MYSQL
- Privilegios 500 de host de MYSQL
- Privilegios 500 de tabla de MYSQL
- Privilegios 502 de base de datos de MYSQL
- Privilegios 502 de usuario de MYSQL
- Privilegios 502 de host de MYSQL
- Privilegios 502 de tabla de MYSQL

Para que las titularidades puedan subir datos desde varios orígenes de datos, el requisito general es que el inicio de sesión, que se utiliza para acceder a la base de datos, pueda leer las tablas utilizadas en la consulta (que está oculta para todas las titularidades).

La siguiente lista detalla los privilegios mínimos necesarios, en la tabla de base de datos (o vista de la tabla de base de datos), para que la titularidad funcione.

Nota: Además de los privilegios necesarios, el usuario debe conectarse a la base de datos de MYSQL para subir los datos.

Las consultas de titularidad para todas las versiones de MySQL a través de MySQL 5.0.1 utilizan este conjunto de tablas: mysql.db mysql.host mysql.tables_priv mysql.user

A partir de MySQL 5.0.2, y para todas las versiones posteriores, las consultas de titularidad utilizan este conjunto de tablas: information_schema.SCHEMA_PRIVILEGES mysql.host information_schema.TABLE_PRIVILEGES information_schema.USER_PRIVILEGES

Si un origen de datos tiene un tipo de base de datos MYSQL, pero no tiene un nombre de BD (consulte Definiciones de orígenes de datos, el nombre de la base de datos bajo Ubicación está en blanco), los datos de subida entrarán en bucle a través de todas las bases de datos MYSQL a las que tenga acceso el usuario.

Titularidades de BD de DB2

Se proporcionan los dominios siguientes para facilitar la carga y la creación de informes en Titularidades de BD de DB2. Cada uno de los siguientes dominios tiene una sola entidad (con el mismo nombre), y hay un informe predefinido para cada dominio. Todos estos dominios están disponibles en las selecciones Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas. Al igual que con otras entidades e informes predefinidos, éstos no se pueden modificar, pero puede clonar y, a continuación, personalizar sus propias versiones de cualquiera de estos informes o dominios. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador Titularidades de BD.

- Privilegios a nivel de columna de DB2 (SELECT, UPDATE, ETC.)
- Privilegios a nivel de base de datos de DB2 (CONNECT, CREATE, ETC.)
- Privilegios a nivel de índice de DB2 (CONTROL)
- Privilegios a nivel de paquete de DB2 (en paquetes de código – BIND, EXECUTE, ETC.)
- Privilegios a nivel de tabla de DB2 (SELECT, UPDATE, ETC.) Resumen de privilegios de DB2

Para que las titularidades puedan subir datos desde varios orígenes de datos, el requisito general es que el inicio de sesión, que se utiliza para acceder a la base de datos, pueda leer las tablas utilizadas en la consulta (que está oculta para todas las titularidades).

La siguiente lista (con cabecera de línea de comentarios) detalla los privilegios mínimos necesarios, en la tabla de base de datos (o vista de la tabla de base de datos), para que la titularidad funcione.

/* Es necesario seleccionar un privilegio para estas tablas/vistas */

GRANT SELECT ON SYSCAT.COLAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.DBAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.INDEXAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.PACKAGEAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.DBAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.TABAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.SCHEMAAUTH TO SQLGUARD;

GRANT SELECT ON SYSCAT.PASSTHRUAUTH TO SQLGUARD;

Titularidades de DB2 z/OS

Se proporcionan los siguientes dominios para facilitar la carga y la creación de informes sobre las Titularidades de BD de DB2 for z/OS.

Privs. de objetos ejecutables de DB2 zOS otorgados a PUBLIC

Privs. de objetos DB2 zOS otorgados a PUBLIC

Privs. del sistema DB2 zOS otorgados a GRANTEE -V8

Privs. del sistema DB2 zOS otorgados a GRANTEE -V9

Privs. del sistema DB2 zOS otorgados a GRANTEE -V10 y superior

Privs. de base de datos de DB2 zOS otorgados a GRANTEE

Privs. de esquema de DB2 zOS otorgados a GRANTEE -V9 y superior

Privs. del esquema de DB2 zOS otorgados a GRANTEE -Sólo V8

Recurso de base de datos DB2 zOS otorgado a GRANTEE

Privs. de objetos DB2 zOS otorgados a GRANTEE

Privs. del sistema DB2 zOS otorgados con GRANT -V8

Privs. del sistema DB2 zOS otorgados con GRANT -V9

Privs. del sistema DB2 zOS otorgados con GRANT -V10 y superior

Recurso de base de datos DB2 zOS otorgado a PUBLIC

Privs. de esquema de DB2 zOS otorgados a PUBLIC

Privs. de base de datos de DB2 zOS otorgados a PUBLIC

Privs. del sistema DB2 zOS otorgados a PUBLIC -V10 y superior

Privs. del sistema DB2 zOS otorgados a PUBLIC -V9

Privs. del sistema DB2 zOS otorgados a PUBLIC -V8

Privs. de objetos de DB2 zOS otorgados con GRANT

Recurso de base de datos de DB2 zOS otorgado con GRANT

Privs. del esquema de DB2 zOS otorgados con GRANT-Sólo V8

Privs. del esquema de DB2 zOS otorgados con GRANT-V9 y superior

Privs. de la base de datos de DB2 zOS otorgados con GRANT

Titularidades de BD de DB2 for i 6.1 y 7.1

Se proporcionan los siguientes dominios para facilitar la carga y la creación de informes sobre las Titularidades de BD de DB2 for i. Cada uno de los siguientes dominios tiene una sola entidad (con el mismo nombre), y hay un informe predefinido para cada dominio. Todos estos dominios están disponibles en las selecciones Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas. Al igual que con otras entidades e informes predefinidos, éstos no se pueden modificar, pero puede clonar y, a continuación, personalizar sus propias versiones de cualquiera de estos informes o dominios. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador Titularidades de BD.

Utilice el script, gdmmonitor-db2-IBMi.sql, para detallar los privilegios mínimos necesarios, en la tabla de base de datos (o vista de la tabla de base de datos), para que la titularidad funcione.

Privilegios de objeto otorgados al receptor de autorización (Tipo de objeto: Esquema, Tabla, Vista, Paquete, Rutina, secuencia, columna, variable global y esquema XML)

Privilegios de objeto otorgados a PUBLIC (Tipo de objeto: Esquema, Tabla, Vista, Paquete, Rutina, secuencia, columna, variable global y esquema XML)

Privilegios de objetos ejecutables otorgados a PUBLIC (Tipo de objeto: paquete y Rutina)

Privilegios de objeto otorgados al receptor de autorización con la OPCIÓN GRANT (Tipo de objeto: Esquema, Tabla, Vista, Paquete, Rutina, secuencia, columna, variable global y esquema XML)

Todos los privilegios de objeto excluyen los esquemas del sistema predeterminados de un grupo Guardium predefinido denominado "Esquemas del sistema excluidos de DB2 for i - informe de titularidad". Añada a este grupo los esquemas que se deben excluir.

Titularidades de BD de SYBASE

Se proporcionan los siguientes dominios para facilitar la carga y la creación de informes en Titularidades de BD de SYBASE. Cada uno de los siguientes dominios tiene una sola entidad (con el mismo nombre), y hay un informe predefinido para cada dominio. Todos estos dominios están disponibles en las selecciones Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas. Al igual que con otras entidades e informes predefinidos, éstos no se pueden modificar, pero puede clonar y, a continuación, personalizar sus propias versiones de cualquiera de estos informes o dominios. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador Titularidades de BD.

- Privilegio de sistema de SYBASE y roles otorgados al usuario incluyendo la opción de Otorgar
- Rol de SYBASE otorgado a privilegios de usuario y sistema otorgado al usuario y al rol incluyendo la opción de Otorgar
- Acceso de objeto de SYBASE por público
- Privilegio de ejecución de SYBASE en el procedimiento, función asignada a Public
- Cuentas de SYBASE con Roles de administración del sistema o de seguridad
- Privilegio de objetos y columnas de SYBASE otorgado con la opción de Otorgar
- Rol de SYBASE otorgado a usuario

Para que las titularidades puedan subir datos desde varios orígenes de datos, el requisito general es que el inicio de sesión, que se utiliza para acceder a la base de datos, pueda leer las tablas utilizadas en la consulta (que está oculta para todas las titularidades).

La siguiente lista (con cabecera de línea de comentarios) detalla los privilegios mínimos necesarios, en la tabla de base de datos (o vista de la tabla de base de datos), para que la titularidad funcione.

/* Es necesario seleccionar un privilegio para estas tablas/vistas */

/* Son necesarios en la base de datos MASTER */

grant select on master.dbo.sysloginroles to sqlguard

grant select on master.dbo.syslogins to sqlguard

grant select on master.dbo.syssrvroles to sqlguard

/*Son necesarios en cada base de datos, incluida MASTER */

grant select on sysprotects to sqlguard

grant select on sysusers to sqlguard

grant select on sysobjects to sqlguard

grant select on sysroles to sqlguard

Si un origen de datos tiene un tipo de base de datos de SYBASE, pero no tiene un nombre de BD (consulte Definiciones de orígenes de datos, el nombre de la base de datos bajo Ubicación está en blanco), los datos de subida entrarán en bucle a través de todas las bases de datos de SYBASE a las que tenga acceso el usuario.

Titularidades de IQ de SYBASE

Versión admitida: sybase IQ 15 y superior.

La siguiente definición de tabla personalizada se crea para subir datos: (puede ignorar el id).

139 | Privilegios del objeto SybaseIQ15 por usuario de BD

140 | Privilegios del objeto SybaseIQ15 por grupo

141 | Autoridad del sistema SybaseIQ15 y grupo otorgados al usuario

142 | Autoridad del sistema de SybaseIQ15 y grupo otorgado a usuario y grupo

143 | Acceso a objetos de SybaseIQ15 por Público

144 | Priv. de ejec. de SybaseIQ15 en func. de proc. a PUBLIC

145 | Grupo de usuarios de SybaseIQ15 con admin. de perms. de DBA etc

146 | Priv. de vista de tabla de SybaseIQ15 otorgada con otorgar

147 | Grupo de SybaseIQ15 otorgado a un usuario y a un grupo

148 | Política de inicio de sesión de SybaseIQ15 para el grupo de usuarios con el inicio de sesión

Las consultas/informes correspondientes son los siguientes: (puede ignorar el id).

597 | Privilegios del objeto SybaseIQ15 por usuario de BD

598 | Privilegios del objeto SybaseIQ15 por grupo

599 | Autoridad del sistema SybaseIQ15 y grupo otorgados al usuario

600 | Autoridad del sistema SybaseIQ15 y grupo otorgados a los usuarios y a los receptores de autorización de los grupos

601 | Acceso a objetos de SybaseIQ15 por Público

602 | Privilegio de ejecución de SybaseIQ15 en el procedimiento y la función para PUBLIC

603 | Grupo de usuarios de SybaseIQ15 con DBA/Admin. perms./Admin. usuarios/Autoridad de base de datos DBA remota

604 | Priv. de vista de tabla de SybaseIQ15 otorgada con otorgar

605 | Grupo de SybaseIQ15 otorgado a un usuario y a un grupo

606 | Política de inicio de sesión de SybaseIQ15 para usuarios y grupos con el valor de la opción de inicio de sesión

Se pueden encontrar en las titularidades de bd con las demás.

==========

Descripción de cada uno: algunos de ellos se explican por sí mismos. Algunos pueden necesitar algunas palabras adicionales:

1 /*

Privilegios de objeto por usuario de base de datos.

Los objetos incluyen: tabla, vistas, procedimiento y funciones.

Estos son los privilegios otorgados sólo a los usuarios, sin incluir el grupo ni la pertenencia en el grupo.

*/

2. /*

Privilegios de objeto por grupo.

Los objetos incluyen: tabla, vistas, procedimiento y funciones.

Estos son privilegios otorgados sólo a grupo.

*/

3 /* Autoridad del sistema y grupo otorgados a los usuarios.

*/

4 /* Autoridad del sistema y grupo otorgados a los usuarios y a los receptores de autorización de los grupos.

*/

5 /* Acceso a objetos mediante público.

Inclusión de tablas, vistas, funciones y procedimientos

*/

6 /* Ejecutar privilegio en procedimientos y funciones otorgados a PUBLIC:

*/

7 /* Usuarios y grupos con DBA, Admin. perms., Admin. usuarios o Autoridad de base de datos DBA remota.

*/

8 /* Privilegios de Tablas y Vistas otorgados con la opción otorgar a usuarios y grupos.

Nota: Este es el único tipo de opción de otorgar permitido en IQ de Sybase. Las rutinas no se pueden otorgar con la opción otorgar.

*/

9 /* Grupo otorgado a usuarios y grupo.

*/

10 /* Política de inicio de sesión asignada a usuario y grupo con valor de opción de inicio de sesión */

Cómo utilizar GuardAPI para añadir un origen de datos a los informes IQ de Sybase

Cómo utilizar GuardAPI para añadir un origen de datos a cada uno de los informes de IQ de Sybase y cómo ejecutarlos.

Consulte los siguientes ejemplos sobre cómo añadir un origen de datos a cada uno de los informes nuevos y, a continuación, ejecutar cada informe.

Añadir un origen de datos para TODOS los informes de titularidad de SybaseIQ

grdapi create_datasource type="Sybase IQ" user=ent password=Guardium123 host=9.70.144.152 name="SybaseIQ15 entitlement6" shared=true owner=admin application=CustomDomain port=2638 dbName=sn5qpuff

Añada un origen de datos a TODOS los informes de titularidad de SybaseIQ

grdapi create_datasourceRef_by_name application=CustomTables objName="SybaseIQ15 Exec priv on proc func to PUBLIC"datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="SybaseIQ15 Group granted to user and group" datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="SybaseIQ15 Login policy for user group with login"datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="SybaseIQ15 Object Access By Public" datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="SybaseIQ15 Object Privileges By DB User" datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="SybaseIQ15 Object Privileges By Group" datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="SybaseIQ15 System Authority And Group Granted To User"datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="SybaseIQ15 System Authority And Group Granted To User And Group"datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="SybaseIQ15 Table View priv granted with grant"datasourceName="SybaseIQ15 entitlement 6"

grdapi create_datasourceRef_by_name application=CustomTablesobjName="SybaseIQ15 User Group With DBA Perms Admin etc"datasourceName="SybaseIQ15 entitlement 6"

Ejecutar TODOS los informes de titularidad de SybaseIQ

grdapi upload_custom_data tableName=SYBASEIQ15_EXEC_PRIV_ON_PROC_FUNC_TO_PUBLIC

grdapi upload_custom_data tableName=SYBASEIQ15_GROUP_GRANTED_TO_USER_AND_GROUP

grdapi upload_custom_data tableName=SYBASE_OBJ_COL_PRIVS_GRANTED_WITH_GRAN

grdapi upload_custom_data tableName=SYBASEIQ15_OBJECT_ACCESS_BY_PUBLIC

grdapi upload_custom_data tableName=SYBASEIQ15_OBJECT_PRIVS_BY_DB_USER

grdapi upload_custom_data tableName=SYBASEIQ15_OBJECT_PRIVILEGES_BY_GROUP

grdapi upload_custom_data

tableName=SYBASEIQ15_SYSTEM_AUTHORITY_AND_GROUP_GRANTED_TO_USER grdapi upload_custom_data

tableName=SYBASEIQ15_SYSTEM_AUTHORITY_AND_GROUP_GRANTED_TO_USER_AND_GROUP grdapi upload_custom_data

tableName=SYBASEIQ15_TABLE_VIEWS_PRIV_GRANTED_WITH_GRANT grdapi upload_custom_data

tableName=SYBASEIQ15_USER_GROUP_WITH_DBA_PERMS_ADMIN_ETC

Titularidades de BD de Informix

Se proporcionan los dominios siguientes para facilitar la carga y la creación de informes en Titularidades de BD de Informix. Cada uno de los siguientes dominios tiene una sola entidad (con el mismo nombre), y hay un informe predefinido para cada dominio. Todos estos dominios están disponibles en las selecciones Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas. Al igual que con otras entidades e informes predefinidos, éstos no se pueden modificar, pero puede clonar y, a continuación, personalizar sus propias versiones de cualquiera de estos informes o dominios. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador Titularidades de BD.

- Privilegios de objetos de Informix mediante la cuenta de base de datos no incluidos la cuenta ni los roles del sistema
- Privilegios, roles y lenguaje a nivel de base de datos de Informix otorgados al usuario, incluida la opción de otorgar
- Privilegios, roles y lenguaje a nivel de base de datos de Informix otorgados al usuario y al rol, incluida la opción de otorgar
- Objeto de Informix otorgado a Public
- Privilegio de ejecución de Informix en el procedimiento y la función de Informix otorgados a Public
- Cuenta de Informix con privilegios de objetos y columnas de Informix de privilegio de DBA otorgados con la opción de Otorgar
- Rol de Informix otorgado a usuario y rol

Para que las titularidades puedan subir datos desde varios orígenes de datos, el requisito general es que el inicio de sesión, que se utiliza para acceder a la base de datos, pueda leer las tablas utilizadas en la consulta (que está oculta para todas las titularidades). La siguiente lista (con cabecera de línea de comentarios) detalla los privilegios mínimos necesarios, en la tabla de base de datos (o vista de la tabla de base de datos), para que la titularidad funcione.

/* Es necesario seleccionar un privilegio para estas tablas/vistas */

Puesto que todos los usuarios tienen privilegios suficientes para los privilegios SELECT del catálogo del sistema, no hay necesidad de otorgar privilegios a ningún usuario. Parece que a Informix no le gusta otorgar el catálogo del sistema a los usuarios. La concesión siguiente se utilizaría normalmente. Pero en este caso, no son necesarios.

grant select on systables to sqlguard;

grant select on systabauth to sqlguard;

grant select on sysusers to sqlguard;

grant select on sysroleauth to sqlguard;

grant select on syslangauth to sqlguard;

grant select on sysroutinelangs to sqlguard;

grant select on sysprocauth to sqlguard;

grant select on sysprocedures to sqlguard;

grant select on syscolauth to sqlguard;

Si un origen de datos tiene un tipo de base de datos de Informix, pero no tiene un nombre de BD (consulte Definiciones de orígenes de datos, el nombre de la base de datos bajo Ubicación está en blanco), los datos de subida entrarán en bucle a través de todas las bases de datos de Informix a las que tenga acceso el usuario.

Titularidades de BD de MSSQL 2000

Se proporcionan los siguientes dominios para facilitar la carga y la creación de informes en Titularidades de BD de MSSQL 2000. Cada uno de los siguientes dominios tiene una sola entidad (con el mismo nombre), y hay un informe predefinido para cada dominio. Todos estos dominios están disponibles en las selecciones Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas. Al igual que con otras entidades e informes predefinidos, éstos no se pueden modificar, pero puede clonar y, a continuación, personalizar sus propias versiones de cualquiera de estos informes o dominios. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador **Titularidades de BD**.

- Privilegios de objetos de MSSQL2000 mediante la cuenta de base de datos no incluido el usuario predeterminado del sistema
- Privilegios de rol/sistema de MSSQL2000 otorgados al Usuario incluida la opción de otorgar
- Roles de MSSQL2000 otorgados a usuario y rol. Privilegios del sistema otorgados a Usuario y Rol incluida la opción de otorgar
- Acceso a objetos de MSSQL2000 por PUBLIC
- Privilegio de ejecución de MSSQL2000 en funciones y procedimientos del sistema a PUBLIC
- Cuentas de base de datos de MSSQL2000 con el rol db_owner y db_securityadmin

- Cuenta de Servidor de MSSQL2000 con sysadmin, serveradmin y security admin /* ejecutar esta titularidad sólo en la base de datos MASTER */
- Privilegios de objetos y columnas de MSSQL2000 otorgados con la opción de otorgar
- Rol de MSSQL2000 otorgado a un usuario y rol

Para que las titularidades puedan subir datos desde varios orígenes de datos, el requisito general es que el inicio de sesión, que se utiliza para acceder a la base de datos, pueda leer las tablas utilizadas en la consulta (que está oculta para todas las titularidades).

La siguiente lista (con cabecera de línea de comentarios) detalla los privilegios mínimos necesarios, en la tabla de base de datos (o vista de la tabla de base de datos), para que la titularidad funcione.

```
/* Es necesario seleccionar un privilegio para estas tablas/vistas */

/* Son necesarios en la base de datos MASTER */

grant select on dbo.syslogins to sqlguard


/*Son necesarios en cada base de datos, incluida MASTER */

grant select on dbo.sysprotects to sqlguard

grant select on dbo.sysusers to sqlguard

grant select on dbo.sysobjects to sqlguard

grant select on dbo.sysmembers to sqlguard
```

Si un origen de datos tiene un tipo de base de datos de MSSQL, pero no tiene un nombre de BD (consulte Definiciones de orígenes de datos, el nombre de la base de datos bajo Ubicación está en blanco), los datos de subida entrarán en bucle a través de todas las bases de datos de MSSQL a las que tenga acceso el usuario.

Titularidades de BD de MSSQL 20005/2008

Se proporcionan los siguientes dominios para facilitar la carga y la creación de informes en Titularidades de BD de MSSQL 2005 o MSSQL 2008. Cada uno de los siguientes dominios tiene una sola entidad (con el mismo nombre), y hay un informe predefinido para cada dominio. Todos estos dominios están disponibles en las selecciones Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas. Al igual que con otras entidades e informes predefinidos, éstos no se pueden modificar, pero puede clonar y, a continuación, personalizar sus propias versiones de cualquiera de estos informes o dominios. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador **Titularidades de BD**.

Nota: Los dominios de titularidad para MSSQL2005 listados a continuación cubren MSSQL2008 también.
Nota: Los objetos de las Series de consulta dinámica NO se mostrarán en xxx_DEPENDENCIES. Un objeto de una serie de SQL EXECUTE IMMEDIATE a la que llama una unidad de programa almacenada no muestra la dependencia. Esta consulta excluye el propietario de esquema definido en el ID de grupo 202 "Dependencies_exclude_schema-MSSQL". El usuario tiene la capacidad de añadir o sustraer el nombre de esquema de este grupo para la consulta de dependencias.

- Privilegios de objetos de MSSQL2005/8 mediante la cuenta de base de datos no incluido el usuario predeterminado del sistema.
- Privilegios de rol/sistema de MSSQL2005/8 otorgados a Usuario
- Privilegios de rol/sistema de MSSQL2005/8 otorgados a usuario y rol incluida la opción de otorgar
- Acceso a objetos de MSSQL2005/8 por PUBLIC
- Privilegio de ejecución de MSSQL2005/8 en procedimientos y funciones del sistema en PUBLIC
- Cuentas de base de datos de MSSQL2005/8 del rol db_owner y db_securityadmin
- Cuenta de servidor de MSSQL2005/8 de sysadmin, serveradmin y security admin /* ejecutar sólo en la base de datos MASTER */
- Privilegios de objetos y columnas de MSSQL2005/8 otorgados con la opción de otorgar
- Rol de MSSQL2005/8 otorgado a un usuario y rol.

Para que las titularidades puedan subir datos desde varios orígenes de datos, el requisito general es que el inicio de sesión, que se utiliza para acceder a la base de datos, pueda leer las tablas utilizadas en la consulta (que está oculta para todas las titularidades).

La siguiente lista (con cabecera de línea de comentarios) detalla los privilegios mínimos necesarios, en la tabla de base de datos (o vista de la tabla de base de datos), para que la titularidad funcione.

```
/* Es necesario seleccionar un privilegio para estas tablas/vistas */

/* Son necesarios en la base de datos MASTER */

grant select on sys.server_principals to sqlguard


/*Son necesarios en cada base de datos incluida MASTER */

grant select on sys.database_permissions to sqlguard

grant select on sys.database_principals to sqlguard

grant select on sys.all_objects to sqlguard
```

grant select on sys.database_role_members to sqlguard

grant select on sys.columns to sqlguard

Si un origen de datos tiene un tipo de base de datos de MSSQL, pero no tiene un nombre de BD (consulte Definiciones de orígenes de datos, el nombre de la base de datos bajo Ubicación está en blanco), los datos de subida entrarán en bucle a través de todas las bases de datos de MSSQL a las que tenga acceso el usuario.

Titularidades de BD de Netezza

Se proporcionan los siguientes dominios para facilitar la carga y la creación de informes en Titularidades de BD de Netezza. Cada uno de los siguientes dominios tiene una sola entidad (con el mismo nombre), y hay un informe predefinido para cada dominio. Todos estos dominios están disponibles en las selecciones Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas. Al igual que con otras entidades e informes predefinidos, éstos no se pueden modificar, pero puede clonar y, a continuación, personalizar sus propias versiones de cualquiera de estos informes o dominios. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador **Titularidades de BD**.

Nota: No hay ninguna traducción del texto de error de BD para Netezza. El error aparece en la descripción de la excepción. Los usuarios pueden clonar/añadir un informe con la descripción de la excepción para Netezza según sea necesario.

- Netezza: Privs. de obj. por nombre de usuario de BD - Privilegios de objetos con o sin la opción de otorgar mediante el nombre de usuario de la base de datos excluida la cuenta ADMIN.
- Netezza: Privs. de admin. por nombre de usuario de BD - Privilegios de administración con o sin la opción de otorgar mediante el nombre de usuario de la base de datos excluida la cuenta ADMIN.
- Grupo/rol de Netezza otorgado a un usuario - Grupo (Rol) otorgado al usuario
- Privs. de obj. de Netezza por grupo - Privilegios de objetos con o sin la opción de otorgar mediante GROUP excluido PUBLIC.
- Privs. de admin. de Netezza por grupo - Privilegios de administración con o sin la opción de otorgar mediante GROUP excluido PUBLIC.
- Netezza: Privs. de admin. por nombre de usuario de BD, grupo - Privilegios de administración con o sin la opción de otorgar mediante nombre de usuario de base de datos, grupo excluida la cuenta ADMIN y el grupo PUBLIC.
- Privs. de obj. de Netezza otorgados - Privilegios de objeto otorgados con o sin la opción de otorgar a PUBLIC.
- Privs. de admin. de Netezza otorgados - Privilegios de administración otorgados con o sin la opción de otorgar a PUBLIC.
- Priv. de admin. global de Netezza para usuarios y grupos - Privilegios de administración globales otorgados a usuarios y grupos excluida la cuenta ADMIN.
- Priv. de obj. global de Netezza para usuarios y grupos - Privilegios de objetos globales otorgados a usuarios y grupos excluida la cuenta ADMIN.

Para que las titularidades puedan subir datos desde varios orígenes de datos, el requisito general es que el inicio de sesión, que se utiliza para acceder a la base de datos, pueda leer las tablas utilizadas en la consulta (que está oculta para todas las titularidades).

La siguiente lista (con cabecera de línea de comentarios) detalla los privilegios mínimos necesarios, en la tabla de base de datos (o vista de la tabla de base de datos), para que la titularidad funcione.

/* Es necesario seleccionar un privilegio para estas tablas/vistas */

/* Este script se debe ejecutar desde la base de datos del sistema */

GRANT SELECT ON SYSTEM VIEW TO sqlguard;

GRANT LIST ON DATABASE TO sqlguard;

GRANT LIST ON USER TO sqlguard;

GRANT LIST ON GROUP TO sqlguard;

GRANT SELECT ON _V_CONNECTION TO sqlguard;

Para las consultas de titularidad de Netezza, se recomienda conectarse a la base de datos SYSTEM, especialmente cuando se otorga el privilegio al usuario que va a ejecutar estos informes. La otorgación del privilegio DEBE tener lugar desde la base de datos SYSTEM o, de lo contrario, el privilegio otorgado sólo tendrá lugar en una base de datos determinada. Cuando el privilegio otorgado tiene lugar desde la base de datos SYSTEM, una característica especial permitirá que el privilegio otorgado se lleve a cabo en todas las bases de datos.

Titularidades de BD de Teradata

Se proporcionan los siguientes dominios para facilitar la carga y la creación de informes en Titularidades de BD de Teradata. Cada uno de los siguientes dominios tiene una sola entidad (con el mismo nombre), y hay un informe predefinido para cada dominio. Todos estos dominios están disponibles en las selecciones Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas. Al igual que con otras entidades e informes predefinidos, éstos no se pueden modificar, pero puede clonar y, a continuación, personalizar sus propias versiones de cualquiera de estos informes o dominios. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador **Titularidades de BD**.

- Privilegios de objetos de Teradata mediante la cuenta de base de datos no incluidos los usuarios predeterminados del sistema.
- Privilegios y roles del sistema de Teradata otorgados a usuarios incluida la opción de otorgar.
- Roles de Teradata otorgados a usuarios y roles incluida la opción de otorgar.
- Roles de Teradata otorgados a usuarios y roles. Privilegios del sistema otorgados a usuarios y roles incluida la opción de otorgar.
- Privilegios de objetos y sistema de Teradata otorgados a público. Tenga en cuenta que el rol no se puede otorgar a público en Teradata.
- Privilegios de ejecución de Teradata en objetos de base de datos del sistema a público.

- Administración del sistema de Teradata, privilegios de administración de seguridad otorgados a usuario y rol.
  Nota: No hay tal rol de Administrador de seguridad ni de sistema en Teradata. El usuario debe crear sus propios roles. Estos son algunos privilegios de sistema importantes que normalmente no se otorgarían a un usuario normal: ABORT SESSION, CREATE DATABASE, CREATE PROFILE, CREATE ROLE,CREATE USER, DROP DATABASE, DROP PROFILE, DROP ROLE, DROP USER, MONITOR RESOURCE, MONITOR SESSION, REPLICATION OVERRIDE, SET SESSION RATE, SET RESOURCE RATE.
- Privilegios de objetos de Teradata otorgados con la opción granted a usuarios. No se incluye DBC ni receptor de autorización = 'All'.

Para que las titularidades puedan subir datos desde varios orígenes de datos, el requisito general es que el inicio de sesión, que se utiliza para acceder a la base de datos, pueda leer las tablas utilizadas en la consulta (que está oculta para todas las titularidades).

La siguiente lista (con cabecera de línea de comentarios) detalla los privilegios mínimos necesarios, en la tabla de base de datos (o vista de la tabla de base de datos), para que la titularidad funcione.

```
/* Es necesario seleccionar un privilegio para estas tablas/vistas */

GRANT SELECT ON DBC.AllRights TO sqlguard;

GRANT SELECT ON DBC.Tables TO sqlguard;

GRANT SELECT ON DBC.AllRoleRights TO sqlguard;

GRANT SELECT ON DBC.RoleMembers TO sqlguard;
```

Titularidades de BD de PostgreSQL

Se proporcionan los siguientes dominios para facilitar la carga y la creación de informes en Titularidades de BD de PostgreSQL. Cada uno de los siguientes dominios tiene una sola entidad (con el mismo nombre), y hay un informe predefinido para cada dominio. Todos estos dominios están disponibles en las selecciones Creador de dominios personalizados/Consulta de dominios personalizados/Creador de tablas personalizadas. Al igual que con otras entidades e informes predefinidos, éstos no se pueden modificar, pero puede clonar y, a continuación, personalizar sus propias versiones de cualquiera de estos informes o dominios. Para ver los informes de titularidad, inicie sesión en el portal de usuario y vaya al separador **Titularidades de BD**.

Hay siete dominios/consultas/informes personalizados de titularidad para PostgreSQL. Son los siguientes (cada uno de ellos se lista con el nombre, la descripción y la nota de Informe):

- Priv. de PostgreSQL en bases de datos otorgadas al rol de usuario público con o sin opción otorgada. Privilegio sobre bases de datos otorgadas a público, usuario y rol con o sin opción otorgada. Ejecútelo en cualquier base de datos, idealmente en PostgreSQL.
- Priv. de PostgreSQL en idioma otorgado al rol de usuario público con o sin opción otorgada. Privilegio sobre el idioma otorgado a público, usuario y rol con o sin la opción otorgada. Ejecútelo por base de datos.
- Priv. de PostgreSQL en esquema otorgado al rol de usuario público con o sin opción otorgada. Privilegio en Esquema otorgado a público, usuario y rol con o sin la opción otorgada. Ejecútelo por base de datos.
- Priv. de PostgreSQL en espacio de tabla otorgado al rol de usuario público con o sin opción otorgada. Privilegio en Espacio de tabla otorgado a público, usuario y rol con o sin la opción otorgada. Ejecútelo en cualquier base de datos, idealmente en PostgreSQL.
- Rol o usuario de PostgreSQL otorgado al usuario o al rol. Rol o usuario otorgado a usuario o rol incluida la opción de otorgar. Ejecútelo una vez en cualquier base de datos. Idealmente PostgreSQL.
- Superusuario de PostgreSQL otorgado a un usuario o rol. Superusuario otorgado a usuario o rol. Ejecútelo una vez en cualquier base de datos. Idealmente PostgreSQL.
- Privs. de sis. de PostgreSQL otorgados a un usuario y a un rol. Privilegios del sistema otorgados a usuario y rol. Ejecútelo una vez en cualquier base de datos. Idealmente PostgreSQL.
- Secuencia de vista de tabla de PostgreSQL y privs. de función otorgados a público. Privilegios de tablas, vistas, secuencia y funciones otorgados a público. Ejecútelo por base de datos. Ejecútelo por base de datos.
- Secuencia de vista de tabla de PostgreSQL y privs. de función otorgados con la opción de otorgar. Privilegios de tablas, vistas, secuencia y privilegios de funciones otorgados al usuario y al rol sólo con la opción de otorgar. Excluir cuenta de PostgreSQL.
- Secuencia de vista de tabla de PostgreSQL y privs. de función otorgados a roles. Privilegios de tablas, vistas, secuencias y funciones otorgados a roles. No se incluye el público. Ejecútelo por base de datos.
- Secuencia de vistas de tabla de PostgreSQL y privs. de funciones otorgados al inicio de sesión. Privilegios de tablas, vistas, secuencia y funciones otorgados a los inicios de sesión. No se incluye el usuario del sistema postgres. Ejecútelo por base de datos.

Nota: A partir de la versión 8.3.6, PostgreSQL no da soporte a la opción grant admin en público. Sólo hay función, sin procedimiento de almacenamiento. No hay soporte para el otorgamiento de columnas, sólo otorgamiento de tabla. Público es un grupo, no un usuario. Público no se muestra en pg_roles. Los únicos privilegios necesarios para ejecutar todas estas consultas es: GRANT CONNECT ON DATABASE PostgreSQL TO username;

Para que las titularidades puedan subir datos desde varios orígenes de datos, el requisito general es que el inicio de sesión, que se utiliza para acceder a la base de datos, pueda leer las tablas utilizadas en la consulta (que está oculta para todas las titularidades).

La siguiente lista (con cabecera de línea de comentarios) detalla los privilegios mínimos necesarios, en la tabla de base de datos (o vista de la tabla de base de datos), para que la titularidad funcione.

```
/* Es necesario seleccionar un privilegio para estas tablas/vistas */
```

/*Esto es necesario en la base de datos POSTGRES*/

grant connect on database postgres to sqlguard;

/*Son necesarios en cada base de datos, incluido POSTGRES (De forma predeterminada, ya se han otorgado a PUBLIC) */

grant select on pg_class to sqlguard;

grant select on pg_namespace to sqlguard;

grant select on pg_roles to sqlguard;

grant select on pg_proc to sqlguard;

grant select on pg_auth_members to sqlguard;

grant select on pg_language to sqlguard;

grant select on pg_tablespace to sqlguard;

grant select on pg_database to sqlguard;

Si un origen de datos tiene un tipo de base de datos PostgreSQL, pero no tiene un nombre de BD (consulte Definiciones de orígenes de datos, el nombre de la base de datos bajo Ubicación está en blanco), los datos de subida entrarán en bucle a través de todas las bases de datos de PostgreSQL a las que tenga acceso el usuario.

Tema principal: Dominios, entidades y atributos

Cómo sacar provecho de los informes predefinidos

En lugar de crear informes personalizados desde cero, aproveche el contenido predefinido en la aplicación Guardium.

Obtenga la información que busca más rápido, accediendo a informes predefinidos disponibles en la aplicación Guardium. Estos informes predefinidos se pueden clonar y personalizar según las necesidades del usuario.

La utilización de los informes predefinidos de Guardium es una recomendación de práctica recomendada, lo que permite a las organizaciones identificar rápida y fácilmente los riesgos de seguridad, como los objetos expuestos inadecuadamente, los usuarios con derechos excesivos y las acciones administrativas no autorizadas. Algunos ejemplos de los muchos informes predefinidos incluyen: cuentas con privilegios del sistema; todos los privilegios de administrador y sistema, que se muestran por usuario y rol; privilegios de objeto por usuario; y todos los objetos con acceso PUBLIC.

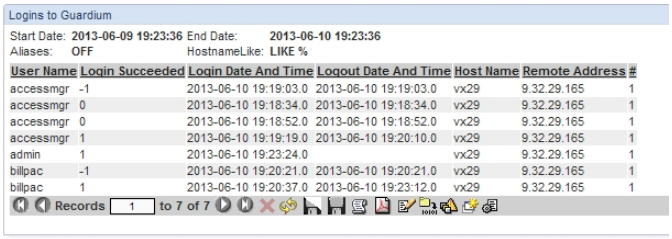
Todos los parámetros y valores se visualizan en todos los informes. Los parámetros y valores se pueden editar mediante Personalizar en la pantalla de informes.

A continuación se describen varios informes de ejemplo.

Inicios de sesión en Guardium

Todos los valores de este informe son de la entidad Inicios de sesión de Guardium. Para el periodo del informe, cada fila del informe lista el Nombre de usuario, Inicio de sesión satisfactorio (1= Satisfactorio, 0=Fallo, -1 =contraseña caducada, -2 = inicio de sesión desde IP distinta), Fecha y hora de inicio de sesión, Fecha y hora de finalización de sesión (que estará en blanco si el usuario todavía no ha finalizado la sesión), Nombre de host, Dirección remota (del usuario) y recuento de inicios de sesión para la fila.

Ubicación de informe: Informes > Supervisión de Sistema Guardium > Inicios de sesión de Guardium


Logins to Guardium

Start Date: 2013-06-09 19:23:36 End Date: 2013-06-10 19:23:36
Aliases: OFF HostnameLike: LIKE %

User Name	Login Succeeded	Login Date And Time	Logout Date And Time	Host Name	Remote Address	#
accessmgr	-1	2013-06-10 19:19:03.0	2013-06-10 19:19:03.0	vx29	9.32.29.165	1
accessmgr	0	2013-06-10 19:18:34.0	2013-06-10 19:18:34.0	vx29	9.32.29.165	1
accessmgr	0	2013-06-10 19:18:52.0	2013-06-10 19:18:52.0	vx29	9.32.29.165	1
accessmgr	1	2013-06-10 19:19:19.0	2013-06-10 19:20:10.0	vx29	9.32.29.165	1
admin	1	2013-06-10 19:23:24.0		vx29	9.32.29.165	1
billpac	-1	2013-06-10 19:20:21.0	2013-06-10 19:20:21.0	vx29	9.32.29.165	1
billpac	1	2013-06-10 19:20:37.0	2013-06-10 19:23:12.0	vx29	9.32.29.165	1

Records 1 to 7 of 7

Tabla 1. Inicios de sesión en Guardium

Dominio	Basado en consulta	Entidad principal
Inicios de sesión de Guardium	Inicios de sesión de Guardium	Inicio de sesión de usuarios de Guardium
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Nombre de host	LIKE	%
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Supervisor de uso de almacenamiento intermedio

Proporciona un amplio conjunto de estadísticas de uso del almacenamiento intermedio.

Ubicación del informe: Informes > Informes operacionales de Guardium > Uso del almacenamiento intermedio empresarial

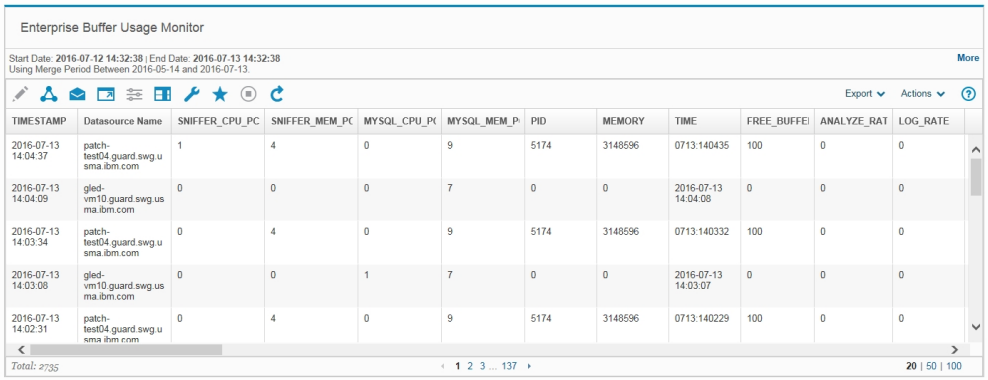


Tabla 2. Supervisor de uso de almacenamiento intermedio

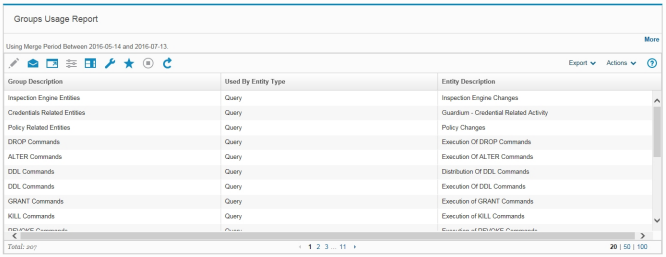
Dominio	Basado en consulta	Entidad principal
Uso de almacenamiento intermedio	Supervisor del uso de almacenamiento intermedio	Supervisor de uso de almacenamiento intermedios de sniffer
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Informe de uso de grupo

Este informe muestra la lista de todos los grupos definidos y todas las entidades que se basan en cada grupo.

Nota: Hay 328 registros disponibles en este informe.

Ubicación del informe: Informes > Supervisión del sistema Guardium > Informe del uso de grupos



Aplicaciones de Guardium

Para cada aplicación de Guardium, cada fila lista un rol de seguridad asignado, o la palabra all, que indica que todos los roles están asignados.

Ubicación del informe: Informes > Informes operativos de Guardium en tiempo real > Todas las aplicaciones de Guardium - Rol

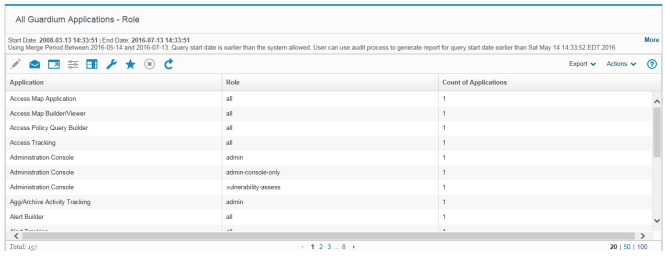


Tabla 3. Aplicaciones de Guardium

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Todas las aplicaciones de Guardium	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -100 Month DAY
Periodo hasta	<=	NOW

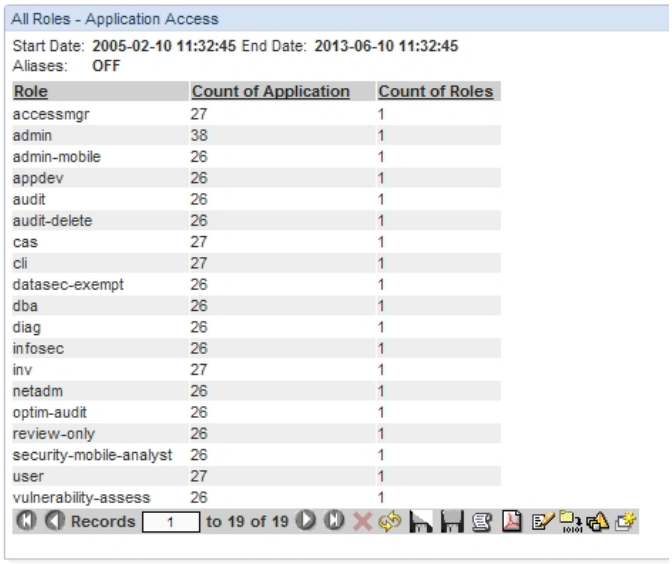
Roles de Guardium

Este panel de menú muestra dos informes: Todos los roles - Acceso a la aplicación y Todos los roles - Usuario.

Todos los roles - Acceso a la aplicación Para cada rol, este informe lista el número de aplicaciones a las que está asignado.

Para listar las aplicaciones a las que está asignado un rol, pulse en el rol y acceda a los detalles en el informe Detalles de registro.

Ubicación del informe: Informes > Supervisión del sistema Guardium > Todos los roles - Acceso a la aplicación



All Roles - Application Access

Start Date: **2005-02-10 11:32:45** End Date: **2013-06-10 11:32:45**
Aliases: **OFF**

Role	Count of Application	Count of Roles
accessmgr	27	1
admin	38	1
admin-mobile	26	1
appdev	26	1
audit	26	1
audit-delete	26	1
cas	27	1
cli	27	1
datasec-exempt	26	1
dba	26	1
diag	26	1
infosec	26	1
inv	27	1
netadm	26	1
optim-audit	26	1
review-only	26	1
security-mobile-analyst	26	1
user	27	1
vulnerability-assess	26	1

Records 1 to 19 of 19

All Roles - User

Start Date: **2005-02-10 11:32:45** End Date: **2013-06-10 11:32:45**
Aliases: **OFF**

Role	Users Belong	# of Roles
accessmgr	1	1
admin	1	1
admin-mobile	0	1
appdev	0	1
audit	0	1

Tabla 4. Todos los roles - Acceso a la aplicación

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Todos los roles - Acceso a la aplicación	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -100 MONTH
Periodo hasta	<=	NOW

Todos los roles - Usuario

Para cada rol, este informe lista el número de usuarios a los que está asignado. Para listar los usuarios a los que está asignado un rol, pulse en el rol y acceda a los detalles en el informe Detalles de registro.

Tabla 5. Todos los roles - Usuario

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Roles - Usuario	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -100 MONTH
Periodo hasta	<=	NOW

Usuarios de Guardium

Lista cada usuario, su fecha de su última actividad y el número de roles asignados. Para cada usuario, puede detallar más hasta el informe de Detalles de registro para ver los roles asignados a ese usuario.

Tabla 6. Usuarios de Guardium

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Rol de usuario	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -100 MONTH
Periodo hasta	<=	NOW

Niveles de utilización de unidad

Los siguientes informes predeterminados proporcionan datos de utilización:

- Utilización de unidad: Muestra el nivel máximo de utilización de unidad de cada unidad en el marco temporal dado. Hay un desglose que muestra detalles para una unidad en todos los periodos dentro del marco temporal del informe.
- Distribución de la utilización de la unidad: Por unidad, este informe visualiza el porcentaje de periodos en el marco temporal del informe con niveles de utilización bajo, medio y alto.
- Umbrales de utilización: Se trata de un informe predefinido que visualiza los valores de umbral altos y bajos de todos los parámetros de utilización de unidad.
- Resumen diario de utilización de la unidad: Proporciona un resumen diario de los datos de utilización de unidad.

Tabla 7. Niveles de utilización de unidad

Dominio	Basado en consulta	Entidad principal
Interno - no disponible	Distribución de utilización de unidad	Niveles de utilización de unidad
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -24 HOUR
Periodo hasta	<=	NOW

- Informes predefinidos
  En el momento de la instalación, el dispositivo Guardium se configura con una serie de informes predefinidos.
- Informes de administrador predefinidos
  En esta sección se proporciona una breve descripción de todos los informes predefinidos en el diseño del administrador predeterminado.
- Informes de usuario predefinidos
  Esta sección proporciona una descripción breve de todos los informes predefinidos en el diseño de usuario predeterminado.
- Común de informes predefinidos
  En esta sección se proporciona una breve descripción de todos los informes predefinidos en los diseños de usuario predeterminado y de administrador predeterminado.

Tema principal: Informes

Informes predefinidos

En el momento de la instalación, el dispositivo Guardium se configura con una serie de informes predefinidos.

Todos los parámetros y valores se visualizan en todos los informes. Los parámetros y valores se pueden editar desde el botón Personalizar en cualquier pantalla de informe.

Utilice la función de búsqueda de ayuda para ir directamente al informe específico. Utilice comillas alrededor de palabras o frases para definir con precisión los términos de búsqueda.

Los informes predefinidos se describen en las páginas siguientes:

- Informes de administración predefinidos Informes de administrador predefinidos Estos son los informes predefinidos disponibles para el usuario administrador.
- Informes predefinidos de Accessmgr (consulte el tema Visión general de la Gestión de acceso): Informes de usuario y de rol; Fuentes de datos permitidas; Servidores permitidos; Bases de datos no asociadas; Fuentes de datos no asociadas.

API para ejecutar un proceso de auditoría desde informes gráficos y tabulares

En la interfaz gráfica de usuario de Guardium, hay un icono (Proceso ad hoc para ejecutar una vez ahora) para invocar una llamada a la GuardAPI, create_ad_hoc_audit_and_run_once.

Se abrirá una ventana con los campos siguientes:

- Direcciones de correo electrónico - Una lista de direcciones de correo electrónico separadas por comas.
- Tipo de contenido para el receptor de correo electrónico: PDF/CSV (un botón de selección 0 - PDF / 1 -CSV)
- Añadir usuario como receptor (recuadro de selección)

El comportamiento de este proceso es el siguiente:

1 - Si es un proceso nuevo, se puede crear uno o varios receptores de correo electrónico en la lista (si hay alguno) con un tipo de contenido tal como se indica en el parámetro emailContentType. También creará un receptor de usuario para el usuario que ha iniciado la sesión (invocando a la API) si el parámetro includeUserReceiver es true.

2 - Si existe un proceso existente, todos los receptores de correo electrónico se eliminarán y se sustituirán por los correos electrónicos de la nueva lista (si hay alguno) con el tipo de contenido tal como se ha definido en el parámetro emailContentType. Si la lista está vacía, se eliminarán todos los destinatarios de direcciones de correo electrónico. Si ya existe un receptor para el usuario, NO se eliminará aunque el valor de includeUserreceiver sea false, pero si el parámetro es true y no existe dicho receptor, se añadirá.

Una vez generado el proceso de auditoría, se ejecutará automáticamente (similar a Ejecutar una vez ahora) y los usuarios deben esperar un elemento de su lista de tareas pendientes para ese proceso de auditoría.

La GuardAPI que crea un proceso de auditoría ad hoc mantendrá los resultados en 7 días (en lugar de 1 día). Los resultados se suprimirán después de 7 días.

Para obtener más información sobre los parámetros, consulte el mandato GuardAPI, create_ad_hoc_audit_and_run_once, en el tema de ayuda Generación de entradas de GuardAPI.

Casos de uso para informes predefinidos

Administrador de base de datos

- Errores de SQL - Un aumento en los errores de SQL puede indicar un ataque de inyección de SQL.

- DDL (verificar cambios de esquema) - Este informe visualiza la IP de cliente a partir de la cual se ha solicitado el DDL, el verbo SQL principal (un mandato DDL específico), y el total de objetos a los que se ha accedido para ese registro.
- Inicios de sesión fallidos - Este informe indica los intentos de acceder a la base de datos con las credenciales de inicio de sesión caducadas.

Responsable de seguridad de información

- Inicios de sesión fallidos - Personas con las credenciales adecuadas que intentan acceder a la base de datos.
- Usuarios finalizados - Usuarios finalizados que intentan acceder a la base de datos.
- Infracciones de política - Usuarios y problemas que infringen las políticas de seguridad.

Auditores

- Informes de conformidad - PCI, SOX, Privacidad de datos
- Flujo de trabajo de conformidad - Muestra las pruebas de los fines de sesión y los procedimientos.

Tema principal: Cómo sacar provecho de los informes predefinidos

Informes de administrador predefinidos

En esta sección se proporciona una breve descripción de todos los informes predefinidos en el diseño del administrador predeterminado.

La selección de informes de la interfaz gráfico de usuario de Guardium tiene cinco secciones:

- Herramientas de configuración de informes;
- Informes operativos de Guardium;
- Informes operativos de Guardium en tiempo real;
- Elementos de configuración de Guardium; y,
- Supervisión del sistema Guardium.

Nota: Si se ha habilitado la seguridad a nivel de datos observados (consulte valores de Perfil global), entonces se filtrará la salida del proceso de auditoría para que los usuarios sólo vean la información de sus bases de datos.

A continuación encontrará una lista de los informes de administrador predefinidos.

S-TAP activos modificados

Esta alerta solo se ejecuta en sistemas de Gestor central (CM). Se muestra el Host S-TAP, la versión de S-TAP, S-TAP cambiado, la indicación de fecha y hora y el recuento.

Tabla 1. S-TAP activos modificados

Dominio	Basado en consulta	Entidad principal
interno - no disponible	S-TAP activos modificados	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	ninguna	ninguna

Inicios de sesión de usuario administrador

Resumen de los inicios de sesión en la base de datos utilizando un nombre de usuario de base de datos definido en el grupo Usuarios administradores. El informe muestra la dirección IP de cliente desde la que el usuario con privilegios administrativos ha iniciado la sesión en la base de datos, el nombre de usuario de la base de datos, el programa fuente, la fecha y hora de inicio de sesión y el total de la sesión para dicho registro.

Tabla 2. Inicios de sesión de usuario administrador

Dominio	Basado en consulta	Entidad principal
Acceso	Inicio de sesión de usuarios de administración	Sesión
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Registro de agregación/archivado

Este informe lista la actividad de agregación de Guardium por tipo de actividad. Cada fila del informe contiene el Tipo de actividad, Hora de inicio, Nombre de archivo, Estado, Comentario, Nombre de host Guardium, Registros depurados, Inicio de periodo, Finalización de periodo y recuento de registros de la fila. Puede limitar la salida estableciendo el parámetro de tiempo de ejecución Nombre de host Guardium, que se establece en % de forma predeterminada (para seleccionar todos los servidores). La columna Registros depurados contiene un recuento de registros depurados sólo cuando el tipo de actividad es Depurar.

Tabla 3. Registro de agregación/archivado

Dominio	Basado en consulta	Entidad principal
Agregación/Exportación/Importación	Registro de agregación/archivado	Registro de agregación/archivado
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 WEEK

Dominio	Basado en consulta	Entidad principal
Periodo hasta	<=	NOW
Nombre de host de Guardium	LIKE	%

Todas las aplicaciones de Guardium - Roles

Este panel de menú muestra dos informes: Todos los roles - Acceso a la aplicación y Todos los roles - Usuario.

Todos los roles - Acceso a la aplicación

Para cada rol, este informe lista el número de aplicaciones a las que está asignado. Para listar las aplicaciones a las que está asignado un rol, pulse en el rol y acceda a los detalles en el informe Detalles de registro.

Tabla 4. Todos los roles - Acceso a la aplicación

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Todos los roles - Acceso a la aplicación	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -100 MONTH
Periodo hasta	<=	NOW

Todos los roles - Usuario

Para cada rol, este informe lista el número de usuarios a los que está asignado. Para listar los usuarios a los que está asignado un rol, pulse en el rol y acceda a los detalles en el informe Detalles de registro.

Tabla 5. Todos los roles - Usuario

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Role - Usuario	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -100 MONTH
Periodo hasta	<=	NOW

Valores de dispositivo

Este informe muestra los valores de configuración de un sistema Guardium. Utilice el informe *valores del dispositivo* para revisar y validar rápidamente los valores de Guardium.

Tabla 6. Valores de dispositivo

Dominio	Basado en consulta	Entidad principal
interno - no disponible	S-TAP activos modificados	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Mostrar alias		Botones de selección (activado, desactivado, predeterminado)
Origen de datos remoto		Menú desplegable

Resumen de los objetos de aplicación

Este informe es un resumen de todas las definiciones en la aplicación Guardium. Por ejemplo, escriba Oracle en el espacio ObjectNameLike en la página de Parámetros de tiempo de ejecución de Objetos de aplicación y encuentre todos los Tipos de objeto y Descripciones de Objeto donde se utiliza Oracle.

Nota: Este informe presenta metadatos y, como tal, no se filtra a través del mecanismo de seguridad a nivel de datos. Estos metadatos podrían incluir información relacionada con la base de datos como, por ejemplo, SID de Oracle.

Tabla 7. Resumen de los objetos de aplicación

Dominio	Basado en consulta	Entidad principal
Objetos de aplicación	Resumen de los objetos de aplicación	Objetos de aplicación
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
ObjectNameLike	%	%
ObjectTypeNameLike	%	%

Clientes de tap aprobados

Sólo se permite que S-TAP específicos se conecten a la aplicación Guardium. Este informe muestra qué S-TAP se ha aprobado y su estado.

Tabla 8. Clientes de tap aprobados

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Clientes de tap aprobados	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Registro del proceso de auditoría

Registro del proceso de auditoría

Este informe muestra un registro de actividad detallado de todas las tareas, incluidas las horas de inicio y finalización. Este informe está disponible a los usuarios administradores a través del separador Supervisor de Guardium. Las tareas de auditoría muestran las horas de inicio y de finalización, aunque el inicio y el final de las clasificaciones y los asesoramientos de seguridad (que van a una cola) es el mismo.

El proceso de auditoría se ha ampliado para la aprobación de filas específicas más allá de una aprobación del usuario a todo el proceso de auditoría. Muestra una lista de lo que aprobado y cuál es el estado de filas específicas.

Utilice este registro de proceso de auditoría para detener los procesos de auditoría. Las tareas sólo se pueden detener si las tareas no se han ejecutado o están en ejecución. Cualquier otra tarea no iniciada no se ejecutará. Los resultados parciales no se entregarán. Si las tareas se han completado, la detención del proceso de auditoría no detendrá el envío de los resultados. La detención del proceso de auditoría se realiza a través de un mandato GrdAPI, invoke api, desde el informe Registro de proceso de auditoría. Para cualquier usuario, sólo muestra la línea que pertenece al usuario (pero sin todos los detalles, sólo las tareas). Los usuarios administradores pueden ver todos los detalles y pueden detener las ejecuciones de cualquier otro usuario. Los usuarios sólo pueden detener sus propias ejecuciones.

Nota:

Detener el proceso de auditoría no cancelará las consultas que se estén ejecutando utilizando un origen remoto. Ninguno de los dos realizará informes en línea que utilicen un origen remoto.

No está soportado para los conjuntos de privacidad y canales de información externos. Esto significa que si se ha iniciado la tarea del conjunto de privacidad o si se ha iniciado el canal de información externo, finalizará incluso si el proceso está detenido (en contraposición a una consulta que se interrumpirá con kill).

ID de registro de proceso de auditoría

Nombre de inicio de sesión

ID de ejecución

Indicación de fecha y hora

ID de proceso de auditoría

Descripción de proceso de auditoría

ID de tarea de auditoría

Descripción de tarea de auditoría

Tipo de suceso

Detalle

Recuento de registro de proceso de auditoría

Parches disponibles

Muestra una lista de parches disponibles. No hay parámetros de tiempo de ejecución, y este dominio de informes es sólo del sistema.

Supervisor de uso de almacenamiento intermedio

Proporciona un amplio conjunto de estadísticas de uso del almacenamiento intermedio. Consulte la descripción de la entidad Utilización del almacenamiento intermedio de sniffer para obtener una descripción de los campos que se listan en este informe.

Tabla 9. Supervisor de uso de almacenamiento intermedio

Dominio	Basado en consulta	Entidad principal
Uso de almacenamiento intermedio	Supervisor del uso de almacenamiento intermedio	Supervisor de uso de almacenamiento intermedios de sniffer
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Despliegue de CAS

Este informe CAS detalla el tipo de base de datos, el nombre de SO, el nombre de host y el tipo de SO.

Tabla 10. Despliegue de CAS

Dominio	Basado en consulta	Entidad principal

Dominio	Basado en consulta	Entidad principal
CAS	Despliegue de CAS	N/D
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Tipo de BD	Like	%
OS_Name	Like	%
Hostname	Like	%
OS_Type	Like	%

Cambios (CAS)

Detalles de cambios de CAS

El propietario lista los cambios en orden de cada elemento supervisado.

Tabla 11. Detalles de cambios de CAS

Dominio	Basado en consulta	Entidad principal
Cambios de CAS	Detalles de cambios de CAS	Configuración de host
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
DB_Type	Like	%
Host_Name	Like	%
Instance_Name	Like	%
Monitored_Item	Like	%
OS_Type	Like	%
Type	Like	%

Datos guardados de CAS

Este informe lista los datos guardados para cada cambio detectado. Este informe se ordena por nombre de host y, a continuación, por la hora de modificación más reciente.

Tabla 12. Datos guardados de CAS

Dominio	Basado en consulta	Entidad principal
Cambios de CAS	Datos guardados de CAS	Datos guardados
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Host_Name	Like	%
Monitored_Item	Like	%
Saved_Data_Id	Like	%

Configuración (CAS)

Instancias de CAS

Este informe lista definiciones de instancias de CAS (una instancia de CAS aplica un conjunto de plantillas a un host de CAS específico). El orden de clasificación predeterminado para este informe es no estándar. Las claves de clasificación son, de mayor a menor: nombre de host (ascendente), instancia (ascendente) y último cambio de estado (descendente).

Tabla 13. Instancias de CAS

Dominio	Basado en consulta	Entidad principal
Configuración de CAS	Instancias de CAS	Detalles de elemento supervisado
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Host_Name	Like	%
OS_Type	Like	%
DB_Type	Like	%
Instance	Like	%

Configuración de instancias de CAS

El informe lista los cambios en la configuración de la instancia de CAS. El orden de clasificación predeterminado para este informe es no estándar. Las claves de clasificación son, de mayor a menor: nombre de host (ascendente), instancia (ascendente) y último cambio de estado (descendente). Puede limitar la salida utilizando cualquiera de los parámetros de tiempo de ejecución, que seleccionan todos los parámetros de forma predeterminada.

Tabla 14. Configuración de instancias de CAS

Dominio	Basado en consulta	Entidad principal
Configuración de CAS	Configuración de instancias de CAS	Detalles de elemento supervisado
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Host_Name	Like	%
OS_Type	Like	%
Template_Id	Like	%

Lista de perfilado de conexión

La Lista de perfilado de conexión es un grupo de todas las conexiones permitidas (la Lista de perfilado de conexión muestra todos los detalles de la conexión).

Tabla 15. Lista de perfilado de conexión

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Lista de perfilado de conexión	Cliente Servidor
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Fecha desde de consulta	>=	NOW -1 DAY
Fecha hasta de consulta	<=	NOW

Conexiones en cuarentena

Las políticas de Guardium se pueden utilizar para terminar o poner en cuarentena conexiones en tiempo real. Utiliza alertas de umbral, basadas en consultas. Consulte el Cuarentena bajo el tema Políticas para obtener instrucciones de configuración.

Tabla 16. Conexiones en cuarentena

Dominio	Basado en consulta	Entidad principal
Cuarentena de conexión	Conexiones en cuarentena	Cuarentena de conexión
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
IP de servidor	LIKE	%
Usuario de BD	LIKE	%
Nombre de servidor	LIKE	%
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Rastreador de CPU

Lista el host TAP de software y el número de unidades CPU en máquinas que ejecutan S-TAP.

Tabla 17. Rastreador de CPU

Dominio	Basado en consulta	Entidad principal
interno - no disponible	no disponible	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
ninguna	n/d	n/d

Uso de CPU

De forma predeterminada, muestra el uso de CPU durante las últimas dos horas. Este informe gráfico está pensado para visualizar solo la actividad reciente. Si modifica los parámetros de tiempo de ejecución Desde y Hasta para incluir un marco temporal mayor, es posible que reciba un mensaje que indica que hay demasiados datos. Utilice un informe tabular para mostrar un periodo de tiempo mayor.

Tabla 18. Uso de CPU

Dominio	Basado en consulta	Entidad principal
Almacenamiento intermedio de sniffer	Uso de CPU	Supervisor de uso de almacenamiento intermedios de sniffer
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -2 HOUR
Periodo hasta	<=	NOW

Bases de datos por tipo/ número de BD por tipo

Tipo de servidor y orígenes de cliente para cada tipo de base de datos supervisada.

Tabla 19. Bases de datos por tipo

Dominio	Basado en consulta	Entidad principal
Acceso	Número de bd por tipo	Cliente/Servidor
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Bases de datos descubiertas

Para el periodo de informe, para cada entidad Puerto descubierto donde el valor de atributo Tipo de BD es NOT LIKE Desconocido, este informe lista la Indicación de fecha y hora de sondeo, IP de servidor, Nombre de host de servidor, Tipo de BD, Puerto, Tipo de puerto y un recuento de Puertos descubiertos por fila.

Tabla 20. Bases de datos descubiertas

Dominio	Basado en consulta	Entidad principal
Descubrimiento automático	Bases de datos descubiertas	Puerto descubierto
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW
PortNotLike	NOT LIKE	Ningún valor predeterminado.

Lista de correlación de usuarios de BD

La correlación entre usuarios de base de datos (invocadores del SQL que originó la infracción) y las direcciones de correo electrónico para las alertas en tiempo real.

Tabla 21. Lista de correlación de usuarios de BD

Dominio	Basado en consulta	Entidad principal
Descubrimiento automático	Lista de correlación de usuarios de BD	Inicio de sesión de usuarios de Guardium
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Usuarios de la BD predeterminados habilitados

Este informe detalla los usuarios predeterminados que se han habilitado después de escanear la base de datos en el grupo de usuarios predeterminados y la lista de servidores proporcionados a la API de escaneo sin credenciales. Cuando se encuentra un usuario habilitado dentro de una base de datos, dicha aparición de base de datos/usuario sólo se notifica una vez. Los escaneos posteriores actualizarán la versión de base de datos y la indicación de fecha y hora de la base de datos. Si un escaneo posterior no encuentra un usuario encontrado previamente, la indicación de fecha y hora permanece inalterada para conservar un historial con la última vez que se encontró habilitado el usuario en una base de datos. Los escaneos que se ejecutan bajo el escucha clasificador y los trabajos enviados (con la API non_credential_scan) se pueden seguir utilizando el informe de Cola de trabajos de Guardium.

Tabla 22. Usuarios de la BD predeterminados habilitados

Dominio	Basado en consulta	Entidad principal
Usuarios de la BD predeterminados habilitados	Usuarios de la BD predeterminados habilitados	Usuarios de la BD predeterminados habilitados
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Orígenes de datos

Lista todos los orígenes de datos definidos: Tipo de origen de datos, Nombre de origen de datos, Descripción de origen de datos, Host, Puerto, Nombre de servicio, Nombre de usuario, Nombre de base de datos, Última conexión, Compartido y Propiedades de conexión.

Puede restringir la salida de este informe utilizando el parámetro de tiempo de ejecución Nombre de origen de datos, que, de forma predeterminada, se establece en "%" para seleccionar todos los orígenes de datos.

Tabla 23. Orígenes de datos

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Orígenes de datos	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Nombre de origen de datos	LIKE	%
Periodo desde	>=	NOW -1 DAY

Dominio	Basado en consulta	Entidad principal
Periodo hasta	<=	NOW

Instancias descubiertas

Este informe de S-TAP detalla la información siguiente:

Indicación de fecha y hora, Host, Protocolo, Mínimo puerto, Máx. de puerto, Puerto BD KTAP, Nombre de instancia, Cliente, Excluir cliente, Nombre proc, Conducto con nombre, Dir instancia BD, Ajuste mem compartida DB2, Posición cliente mem compartida DB2, Tamaño mem compartida DB2.

Tabla 24. Instancias descubiertas

Dominio	Basado en consulta	Entidad principal
Excepción	Instancias descubiertas	Excepción
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Registro de extracción de despensa de datos

Una despensa de datos es un tipo de almacén de datos. Un almacén de datos agrega y organiza los datos de una forma genérica que se pueden utilizar posteriormente para informes y análisis. Una despensa de datos empieza por un análisis de datos definido por el usuario y hace énfasis en el cumplimiento de las demandas específicas del usuario en términos de contenido, presentación y facilidad de uso.

El programa de extracción de la despensa de datos se ejecuta por lotes de acuerdo con la planificación especificada. Resume los datos por horas, días, semanas o meses según la granularidad solicitada y, a continuación, guarda los resultados en una tabla nueva en la base de datos de analíticas de Guardium.

A continuación, los datos son accesibles para los usuarios a través de los programas de utilidad de Informes estándar y Proceso de auditoría e, igualmente, para cualquier otra Entidad/ Dominio tradicional. Los datos de extracción de la despensa de datos están disponibles bajo el dominio DM. El nombre de entidad se establece de acuerdo con el nuevo nombre de tabla especificado para los datos de la despensa de datos. Utilizando el Creador de consultas y el Creador de informes, los usuarios pueden clonar la consulta predeterminada y editar la consulta e informe, generar portlets y añadirlos a un panel.

El registro de extracción está formado por: Nombre de despensa de datos, IP de recopilador, IP de servidor, desde fecha, hasta fecha, ID, ejecución iniciada, ejecución finalizada, número de registros, estado, código de error.

Registro de exportación/importación de definiciones

Este informe lista la actividad de importación/exportación de Guardium por tipo de actividad. Cada fila del informe contiene Tipo de actividad, Hora de inicio, Nombre de archivo, Estado, Comentario y el recuento de registros de la fila.

Tabla 25. Registro de exportación/importación de definiciones

Dominio	Basado en consulta	Entidad principal
Agregación/Archivado	Registro de definiciones de exportación-importación	Registro de agregación/archivado
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Solicitudes descartadas

Solicitudes de seguimiento descartadas por un motor de inspección (Descripción de excepción = Solicitud de base de datos descartada). En situaciones muy raras y de gran volumen, es posible que se pierdan algunas solicitudes. Si esto ocurre, las sesiones desde las que se han perdido las solicitudes aparecen listadas en el informe de Solicitudes descartadas.

Tabla 26. Solicitudes descartadas

Dominio	Basado en consulta	Entidad principal
Excepciones	Solicitudes descartadas	Excepción
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Recuento de excepciones

Para el periodo del informe, el número total de excepciones registradas.

Tabla 27. Recuento de excepciones

Dominio	Basado en consulta	Entidad principal
Excepciones	Recuento de excepciones	Excepción

Dominio	Basado en consulta	Entidad principal
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Vista de S-TAP de empresa (detallada)

Consulte la Información de S-TAP (Gestor central) para obtener información sobre este informe.

Historial de asociación de S-TAP de empresa

Historial de asociación de S-TAP de empresa informa del tiempo que S-TAP informó a un sistema de Guardium específico en el entorno del Equilibrador de carga.

Vista de S-TAP de empresa

Consulte la Información de S-TAP (Gestor central) para obtener información sobre este informe.

Exportación de datos confidenciales a descubrimiento

Guardium e InfoSphere Discovery tienen mecanismos para la clasificación de datos confidenciales.

Se proporciona una interfaz bidireccional para transferir los datos confidenciales desde Guardium a InfoSphere Discovery y desde InfoSphere Discovery a Guardium.

Estos datos se transferirán a través de archivos CSV. Consulte Correlación de datos externos (Interfaz bidireccional) para obtener más información.

Tabla 28. Exportación de datos confidenciales a descubrimiento

Dominio	Basado en consulta	Entidad principal
Interno - no disponible	Exportación de datos confidenciales a descubrimiento	Resultados del proceso de clasificación
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -3 HOURS
Periodo hasta	<=	NOW
Descripción de regla	LIKE	
Esquema	LIKE	

Supervisor de uso de almacenamiento intermedio de empresa

Este informe muestra el uso agregado del almacenamiento intermedio de sniffer de todas las unidades gestionadas. Existe una necesidad de establecer la planificación para la subida. Consulte la descripción de la entidad Utilización del almacenamiento intermedio de sniffer para obtener una descripción de los campos que se listan en este informe.

Tabla 29. Supervisor de uso de almacenamiento intermedio de empresa

Dominio	Basado en consulta	Entidad principal
Uso de almacenamiento intermedio de empresa	Uso de almacenamiento intermedio de empresa	Uso de almacenamiento intermedio de sniffer
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Cola de trabajos de Guardium

Muestra la cola de trabajos de Guardium. Anteriormente se denominada Cola de trabajos de clasificador/asesoramiento. Para cada trabajo, lista el ID de ejecución de proceso, Tipo de proceso, Estado, ID de proceso de trabajo de Guardium, ID de resultado de informe, Descripción de trabajo de Guardium, Descripción de tarea de auditoría, Tiempo de cola, Hora de inicio, Hora de finalización y Orígenes de datos.

Tabla 30. Cola de trabajos de Guardium

Dominio	Basado en consulta	Entidad principal
Interno - no disponible	Cola de trabajos de Guardium	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Descripción de trabajo	LIKE	%
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

La cola de trabajos

Los asesoramientos y las clasificaciones se ejecutan en procesos separados en una cola de trabajos. Los trabajos se ponen en cola y mantienen su estado mientras un escucha sondea periódicamente la cola en busca de trabajos en espera para su ejecución.

Deteniéndose

Cuando se pulsa con el botón derecho del ratón para profundizar sobre los trabajos en ejecución, hay una opción para detener el trabajo en ejecución y para cancelarlo. El trabajo no se puede reiniciar en este punto.

Parando

Los trabajos en ejecución se supervisan para reducir el número de trabajos colgados que podrían hacer que la cola de trabajos se desbordase. Si un trabajo está inactivo durante 30 minutos, se termina y se reinicia el escucha, deteniendo de forma efectiva el trabajo. Antes de que se reinicie el escucha, se llama a un proceso de limpieza (cleaner) para ejecutarlo, el estado cambia de EN EJECUCIÓN a PARADO y, a continuación, se reinicia el escucha. Un estado de PARADO significa que el trabajo no se ha podido ejecutar hasta el final.

Volver a enviar

A veces, el escucha se reinicia por razones distintas al cuelgue de los trabajos, por ejemplo, al rearrancar la máquina. Cuando el proceso de limpieza (cleaner) para los trabajos en ejecución, verá si el trabajo ha respondido en los últimos 8 minutos. Si es así, el trabajo se copiará y esa copia se volverá a enviar a la cola de trabajos. La parada original detenida se seguirá visualizando en la cola, y todavía tendrá disponibles los resultados que hubiese podido procesar.

Supervisión

El mecanismo por el que los trabajos mantienen su estado activo es actualizando la indicación de fecha y hora en el registro de la cola de trabajos. Es importante tener en cuenta que el registro de la cola de trabajos se utiliza para todo el trabajo. Cada prueba de asesoramiento o regla de clasificador interactúa con la indicación de fecha y hora para su proceso padre, y no tiene indicaciones de fecha y hora individuales supervisadas.

El clasificador actualizará su indicación de fecha y hora antes de probar cada regla y después de cada operación de SQL. Por ejemplo, si el clasificador está escaneando los datos en una base de datos que da soporte a la paginación, actualizará la indicación de fecha y hora después de que cada lote de datos se haya traído desde la base de datos. Esto se debe a que, en función del estado de la base de datos de destino, el clasificador tiene la posibilidad de invocar algunas consultas de larga duración que se limitarán a 30 minutos de ejecución.

Los asesoramientos modifican la indicación de fecha y hora después de que se evalúe cada prueba en el asesoramiento. La mayoría de las pruebas de asesoramiento se ejecutan en unos segundos o menos.

Pruebas observadas

La excepción a las pruebas de asesoramiento de relativamente larga ejecución es la categoría de pruebas asesoramiento observadas. Estas pruebas se basan en consultas e informes que utilizan los datos de internos de sniffer en el dispositivo Guardium y se pueden ejecutar durante periodos más largos de tiempo y no pueden actualizar la indicación de fecha y hora mientras están en proceso. Por lo tanto, las pruebas de asesoramiento observadas tienen establecidas sus indicaciones de fecha y hora dos horas en el futuro cuando éstas se inician, lo que esencialmente les da dos horas y treinta minutos para ejecutarse completamente. Esto puede resultar confuso al mirar la cola de trabajos y ver la indicación de fecha y hora establecida en una hora futura. Al igual que cualquier otra prueba de asesoramiento, cuando la prueba observada finalice, se actualizará la indicación de fecha y hora. Si la siguiente prueba es una prueba observada, la indicación de fecha y hora se establecerá de nuevo dos horas en el futuro. De lo contrario, la indicación de fecha y hora se establecerá en la hora actual.

Estado de los clientes de GIM

Muestra una lista de clientes de GIM.

Tabla 31. Estado de los clientes de GIM

Dominio	Basado en consulta	Entidad principal
Estado de los clientes de GIM	Estado de los clientes de GIM	Clientes GIM
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Nombre de cliente	%	N/D
SO de cliente	%	N/D

Lista de sucesos de GIM

Muestra una lista de sucesos de GIM.

Tabla 32. Lista de sucesos de GIM

Dominio	Basado en consulta	Entidad principal
Sucesos de GIM	Sucesos de GIM	Sucesos de GIM
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Módulos instalados de GIM

Muestra una lista de los módulos GIM instalados.
Nota: Este informe muestra los módulos que se han asociado con el host. Si se ha asignado un módulo a un host, la versión asignada aparecerá en este informe, incluso si el módulo aún no se ha planificado o instalado. Para comprobar el módulo instalado actualmente, revise el informe de Estado del cliente de GIM.

Tabla 33. Módulos instalados de GIM

Dominio	Basado en consulta	Entidad principal

Dominio	Basado en consulta	Entidad principal
Base instalada GIM	Base instalada GIM	Instalados de GIM
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
ninguna	no aplicable	no aplicable

Informe de uso de grupo

Muestra la lista de todos los grupos definidos y todas las entidades que se basan en cada grupo.

Excepciones de API de Guardium

Muestra una indicación de fecha y hora y una descripción de todas las excepciones de GuardAPI. Son trabajos donde el ID de tipo de excepción es GUARD_API_EXCEPTION.

Tabla 34. Excepciones de API de Guardium

Dominio	Basado en consulta	Entidad principal
Excepción	Excepciones de API de Guardium	Excepción
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Aplicaciones de Guardium

Para cada aplicación de Guardium, cada fila lista un rol de seguridad asignado, o la palabra Todos, que indica que todos los roles están asignados.

Tabla 35. Aplicaciones de Guardium

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Todas las aplicaciones de Guardium	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -100 Month DAY
Periodo hasta	<=	NOW

Detalles de grupo de Guardium

Para el periodo del informe, cada fila del informe lista un miembro del grupo. Las columnas contienen la siguiente información: Descripción de grupo, Tipo de grupo, Subtipo de grupo, Indicación de fecha y hora (desde la entidad Miembro de grupo), Miembro de grupo y el recuento de entidades Miembro de grupo para la fila. El valor de la indicación de fecha y hora se establece en la hora actual siempre que se actualice el registro.

Puede restringir la salida de este informe utilizando los parámetros de tiempo de ejecución, ambos se utilizan con el operador LIKE y un valor predeterminado de %, que selecciona todos los valores.

Tabla 36. Detalles de grupo de Guardium

Dominio	Basado en consulta	Entidad principal
Grupo	Detalles de grupo de Guardium	Miembro de grupo
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Descripción de grupo	LIKE	%
Tipo de grupo	LIKE	%
Periodo desde	>=	NOW -100 MONTH
Periodo hasta	<=	NOW

Usuarios de Guardium

Lista cada usuario, su fecha de su última actividad y el número de roles asignados. Para cada usuario, puede detallar más hasta el informe de Detalles de registro para ver los roles asignados a ese usuario.

Tabla 37. Usuarios de Guardium

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Rol de usuario	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -100 MONTH
Periodo hasta	<=	NOW

Historial de hosts (CAS)

Historial de hosts de CAS

Este informe lista los sucesos de host de CAS. El orden de clasificación predeterminado para este informe es no estándar. Las claves de clasificación son, de mayor a menor: nombre de host (ascendente), hora de suceso e instancia (descendente).

Tabla 38. Historial de hosts de CAS

Dominio	Basado en consulta	Entidad principal
Historial de hosts de CAS	Historial de hosts de CAS	Suceso de host
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Host_Name	Like	%
OS_Type	Like	%
Event_Type	Like	%

Motores de inspección inactivos

Lista todos los motores de inspección inactivos.

Tabla 39. Motores de inspección inactivos

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Motores de inspección inactivos	Cabecera de verificación de S-TAP
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Fecha desde de consulta	>=	NOW -3 HOUR
Fecha hasta de consulta	>=	NOW

S-TAP inactivos desde

Muestra una lista de todos los S-TAP definidos en el sistema. Tiene un solo parámetro de tiempo de ejecución: Periodo desde, que ahora se establece en -1 horas de forma predeterminada. Utilice este parámetro para controlar cómo desea definir la inactividad. Este informe contiene las mismas columnas de datos que el informe de Estado de S-TAP más un recuento para cada fila del informe.

Tabla 40. S-TAP inactivos desde

Dominio	Basado en consulta	Entidad principal
interno - no disponible	S-TAP inactivos desde	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 HOUR

Parches instalados

Muestra una lista de los parches instalados. No hay parámetros de tiempo de ejecución, y este dominio de informes es sólo del sistema.

Tabla 41. Parches instalados

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Parches instalados	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
ninguna	no aplicable	no aplicable

Inicios de sesión para Guardium

Todos los valores de este informe son de la entidad Inicios de sesión de Guardium. Para el periodo del informe, cada fila del informe lista el Nombre de usuario, Inicio de sesión satisfactorio (1= Satisfactorio, 0=Fallo), Fecha y hora de inicio de sesión, Fecha y hora de finalización de sesión (que estará en blanco si el usuario todavía no ha finalizado la sesión), Nombre de host, Dirección remota (del usuario) y recuento de inicios de sesión para la fila.

Tabla 42. Inicios de sesión para Guardium

Dominio	Basado en consulta	Entidad principal
Inicios de sesión de Guardium	Inicios de sesión de Guardium	Inicio de sesión de usuarios de Guardium
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Nombre de host	LIKE	%
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Alertas en tiempo real registradas

Para el periodo del informe, el número total de alertas de tiempo real registradas, listadas según la descripción de la regla.

Tabla 43. Alertas en tiempo real registradas

Dominio	Basado en consulta	Entidad principal
Infracciones de política	Alertas en tiempo real registradas	Infracción de regla de política
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Alertas de umbral registradas

Para el periodo del informe, el número total de alertas de umbral registradas.

Tabla 44. Alertas de umbral registradas

Dominio	Basado en consulta	Entidad principal
Alerta	Alertas registradas	Detalles de alerta de umbral
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Recopiladores de registro (solo válido desde una unidad de agregación)

El informe de Recopiladores de registro aparece bajo el separador Supervisor diario y sólo es válido en una unidad de agregación. Este informe muestra el número de sesiones por IP de servidor, por recopilador y por día. Por ejemplo: el 19 de mayo, el agregador núm. 1 recopiló 100 sesiones para el servidor 192.168.x.x1, 50 sesiones para el servidor 192.168.x.x2; el agregador núm. 2 recopiló 30 sesiones para el servidor 192.168.x.x3, 90 sesiones para el servidor 192.168.x.x4; etc.

Tabla 45. Recopiladores de registro

Dominio	Basado en consulta	Entidad principal
Excepciones	Recopiladores de registro	Recopiladores de registro
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Unidades gestionadas (Gestor central)

El informe empresarial en un Gestor central que muestra las unidades gestionadas activas. Utilice este informe en una alerta estadística para enviar un correo electrónico a un ADMIN siempre que una unidad gestionada esté inactiva.

Tabla 46. Unidades gestionadas (Gestor central)

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Unidades gestionadas	Unidades gestionadas
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Nombre de host	LIKE	%
Origen de datos remoto		Menú desplegable
Mostrar alias		Botones de selección (activado, desactivado, predeterminado)

Número de procesos de auditoría activos

Número de procesos de auditoría de Guardium activos. Cuando se utiliza la gestión central, este informe sólo contiene datos en el Gestor central y está vacío en todas las unidades gestionadas (se visualiza el mensaje estándar, No se han encontrado datos para la consulta solicitada). No hay parámetros de tiempo de ejecución para este informe.

Tabla 47. Número de procesos de auditoría activos

Dominio	Basado en consulta	Entidad principal
Proceso de auditoría	Número de procesos activos	Proceso de auditoría
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
ninguna	no aplicable	no aplicable

Revisiones del proceso de auditoría pendientes

Número de procesos de auditoría de Guardium pendientes, listados por usuarios de Guardium.

Tabla 48. Revisiones del proceso de auditoría pendientes

Dominio	Basado en consulta	Entidad principal
Proceso de auditoría	Revisiones del proceso de auditoría pendientes	Resultados de tarea de listas de tareas pendientes
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
ninguna	no aplicable	no aplicable

Registro de cambio de host Guardium primario

Registro de cambios de host primarios para S-TAP. El host primario es la unidad de Guardium a la que el S-TAP envía los datos. Cada línea del informe lista el Host S-TAP, Nombre de host Guardium, Periodo de inicio y Periodo de finalización.

Tabla 49. Registro de cambio de host Guardium primario

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Registro de cambio de host de SGuard primario	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Atributos y entidades de consulta

Este informe lista todas las entidades y atributos de los informes de Guardium y se ha creado para simplificar el enlace entre los atributos de Guardium y las llamadas de GuardAPI.

Utilice también este informe para invocar a create_constant_attribute, create_api_parameter_mapping, delete_api_parameter_mapping o list_param_mapping_for_function.

Tabla 50. Atributos y entidades de consulta

Dominio	Basado en consulta	Entidad principal
Cualquiera de los dominios para la creación de informes de Guardium	Cualquiera de las entidades para el dominio de informes	Cualquiera de los atributos dentro de la entidad
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Nombre de informe Like Si <> '%' solo mostrará el dominio/entidad y los atributos utilizados por informes que coincidan con el nuevo parámetro. Si es '%', entonces se visualizarán todos los dominios, consultas y atributos(incluidos aquellos que no son utilizados por ningún informe).	no aplicable	no aplicable

Estadísticas de reproducción

Este informe muestra las Estadísticas de reproducción para Fecha de inicio/finalización de ejecución, Nombre de configuración; Nombre de configuración de planificación; Estado de trabajo; Descripción de estadísticas; ID de sesión; Consultas satisfactorias; Consultas fallidas; Total consultas; Tipo; Tareas activas/en espera/completadas.

Tabla 51. Estadísticas de reproducción

Dominio	Basado en consulta	Entidad principal
Seguimiento de resultados de reproducción	Estadísticas de reproducción	Estadísticas de resultado de reproducción
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Fecha desde de consulta	>=	NOW -1 DAY
Fecha hasta de consulta	<=	NOW
Sesión	>=	N/D
Sesión	<=	N/D

Resumen de reproducción

Para el periodo del informe, una medida de las consultas que finalizaron de forma satisfactoria o que fallaron. Es necesario seleccionar Consulta fallada o Consulta satisfactoria en la Configuración de reproducción.

Tabla 52. Resumen de reproducción

Dominio	Basado en consulta	Entidad principal

Dominio	Basado en consulta	Entidad principal
Reproducir resultados	Resumen de reproducción	Reproducir resultados
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Fecha desde de consulta	>=	NOW -1 DAY
Fecha hasta de consulta	<=	NOW
Estado de resultados	%	N/D
Nombre de configuración planificada	%	N/D

Datos restaurados

Este informe tiene dos columnas: RESTORED_DAY y EXPIRATION_DATE. Cuando el usuario restaura los datos desde un archivador, esta tabla se cumplimenta de acuerdo a los datos restaurados y la duración especificada para mantener estos datos. El proceso de depuración consulta esta tabla para determinar los datos que es posible depurar y limpia los registros que han caducado. RESTORED_DAY es la fecha en que se restauraron los datos y que debe estar en el pasado. EXPIRATION_DATE es la fecha en la que se depurarán estos datos y que debe estar en el futuro.

Tabla 53. Datos restaurados

Dominio	Basado en consulta	Entidad principal
Datos restaurados	Datos restaurados	Datos restaurados
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -10 DAY
Periodo hasta	<=	NOW +10 DAY

Velocidad de solicitudes

De forma predeterminada, muestra la velocidad de las solicitudes durante las últimas dos horas. Este informe gráfico está pensado para visualizar solo la actividad reciente. Si modifica los parámetros de tiempo de ejecución para incluir un marco temporal mayor, es posible que reciba un mensaje que indica que hay demasiados datos. Utilice un informe tabular para mostrar un periodo de tiempo mayor.

Tabla 54. Velocidad de solicitudes

Dominio	Basado en consulta	Entidad principal
Almacenamiento intermedio de sniffer	Velocidad de solicitudes	Supervisor de uso de almacenamiento intermedios de sniffer
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -2 HOUR
Periodo hasta	<=	NOW

Conexiones inesperadas

Este informe sólo está disponible cuando la opción de Hunter está habilitada en servidores Unix. La opción Hunter sólo se utiliza cuando se utiliza el método de supervisión Tee. Este informe lista todos los procesos locales que han evitado que S-TAP se conecte a la base de datos.

Tabla 55. Conexiones inesperadas

Dominio	Basado en consulta	Entidad principal
Conexiones inesperadas	Conexiones inesperadas	Conexiones inesperadas
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Excepciones de trabajos planificados

Visualiza una indicación de fecha y hora y la descripción de cada excepción de trabajo planificado (incluidos los errores de asesoramiento). Estos son trabajos donde el Id de tipo de excepción es uno de los siguientes: SCHED_JOB_EXCEPTION, ASSESSMENT_EXCEPTION o ASMT_ERROR.

Tabla 56. Excepciones de trabajos planificados

Dominio	Basado en consulta	Entidad principal
Almacenamiento intermedio de sniffer	Uso de CPU	Uso de almacenamiento intermedio de sniffer
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -2 HOUR
Periodo hasta	<=	NOW

Trabajos planificados

Muestra la lista de trabajos planificados actualmente.

Tabla 57. Trabajos planificados

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Trabajos planificados	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
ninguna	no aplicable	no aplicable

Recuento de sesiones

Para el periodo del informe, el número total de sesiones distintas abiertas.

Tabla 58. Recuento de sesiones

Dominio	Basado en consulta	Entidad principal
Acceso	Recuento de sesiones	Sesión
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Recuento de SQL

Para el periodo del informe, el número de mandatos SQL distintos emitidos.

Tabla 59. Recuento de SQL

Dominio	Basado en consulta	Entidad principal
Acceso	Recuento de SQL	SQL
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Historial de cambio de configuración de S-TAP

Este informe sólo se visualiza cuando se añade o cambia un motor de inspección. Lista los cambios de configuración de S-TAP - cada cambio en el motor de inspección se visualizará en una fila distinta. Cada fila lista el Host de S-TAP, Tipo de servidor de BD, Puerto BD desde, Puerto BD hasta, IP de cliente de BD, Máscara de cliente de BD e Indicación de fecha y hora del cambio.

Tabla 60. Historial de cambio de configuración de S-TAP

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Historial de cambio de configuración	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Estado de S-TAP

Visualiza información de estado de cada motor de inspección definido en cada host de S-TAP. Este informe no tiene parámetros de fecha Desde fecha y Hasta fecha, ya que informa del estado actual. Cada fila en el informe lista el Host de S-TAP, Tipo de servidor de BD, Estado, Última respuesta, Nombre de host primario, Indicadores de Sí/No para los siguientes atributos: KTAP instalado, TEE instalado, Controlador de memoria compartida instalado, Controlador de memoria compartida de DB2 instalado, Controlador de conductos con nombre instalado y Servidor aplicaciones instalado. Además, lista el Hunter DBS.

Nota: El Controlador de memoria compartida de DB2 ha sido reemplazado por la característica DB2 Tap.

Tabla 61. Estado de S-TAP

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Estado de S-TAP	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
ninguna	n/d	n/d

Verificación de S-TAP

Lista todos los resultados de las verificaciones de S-TAP.

Tabla 62. Verificación de S-TAP

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Verificación de S-TAP	Cabecera de verificación de S-TAP
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Fecha desde de consulta	>=	NOW -3 HOUR
Fecha hasta de consulta	>=	NOW

Sucesos de S-TAP

Utilice este informe para obtener información sobre el S-TAP (de la tabla SOFTWARE_TAP_EVENT en la base de datos interna).

Tabla 63. Sucesos de S-TAP

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Sucesos de S-TAP	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Tipo de suceso	LIKE	%
Tipo de host	LIKE	%
Periodo desde	>=	NOW -3 DAY
Periodo hasta	<=	NOW

Información de S-TAP (Gestor central)

Informe: Consulte los informes de S-TAP. En el Gestor central, está disponible un informe adicional, Información de S-TAP. Este informe supervisa los S-TAP de todo el entorno. Suba estos datos utilizando el Creador de tablas personalizadas.

La información de S-TAP es un dominio personalizado predefinido que contiene la entidad Información de S-TAP y que no es posible modificar como los dominios de titularidad.

Al definir una consulta personalizada, vaya a la página de subir y pulse en Comprobar/Reparar para crear la tabla personalizada en la base de datos CUSTOM, de lo contrario, guardar consulta no la validará. Esta tabla se carga automáticamente desde todos los orígenes remotos. Un usuario no puede seleccionar los orígenes remotos que se utilizarán, se extraen de todos ellos.

Basándose en esta tabla personalizada y en este dominio personalizado, hay dos informes:

Vista de S-TAP de empresa, desde el Gestor central, información sobre un S-TAP activo en un recopilador y/o unidad gestionada (Si hay duplicados para el mismo motor de S-TAP, uno activo y el otro inactivo, el informe solo utilizará el activo).

La vista de S-TAP de empresa detallada, muestra desde el Gestor central, información de todos los S-TAP activos e inactivos en todos los recopiladores y/o unidades gestionadas.

Si la vista S-STAP de empresa y la vista S-TAP de empresa detallada tienen el mismo aspecto, es porque sólo hay un S-TAP en una unidad gestionada que se está visualizando. La vista S-TAP de empresa detallada tendrá un aspecto distinto si hay más S-TAP y más unidades gestionadas implicadas.

Estos dos informes se pueden elegir desde el separador de supervisión de TAP en un sistema autónomo, pero no visualizarán información.

Alerta: Consulte Visualización de una definición de proceso de auditoría por alerta: Motores de inspección y S-TAP - alerta de las actividades relacionadas con el motor de inspección y la configuración de S-TAP

Última respuesta de S-TAP

El informe y la consulta predefinidas están disponibles, pero no se añaden a ningún panel.

La consulta/informe muestra Todos los hosts de S-TAP y la última respuesta (latido) enviada por cada host.

El objetivo de esta consulta es ser capaz de definir una alerta que se desencadenará cuando un S-TAP en un host no haya respondido durante un periodo de tiempo determinado.

Los parámetros de entrada son: Última respuesta desde y Última respuesta a.

Por ejemplo, cuando se ejecuta con Última respuesta desde = NOW -5 DAYS y Última respuesta a = NOW - 3 HORAS, visualizará el nombre de host y la hora de la última respuesta de aquellos hosts que han enviado la última respuesta en los últimos 5 días, pero que no han respondido en las últimas 3 horas.

Supervisor de estado de S-TAP

Para cada informe de S-TAP para este dispositivo Guardium, este informe identifica Host de S-TAP, Versión de S-TAP, Tipo de servidor de BD, Estado (activo o inactivo), Última respuesta recibida (fecha y hora), Nombre de host primario e indicadores de verdadero/falso para: KTAP, TEE, Memoria compartida de servidor MS SQL, Memoria compartida de DB2, Supervisión TCP local, Uso de conductos con nombres y cifrado.

Este informe no tiene parámetros de tiempo de ejecución y se basa en una consulta solo de sistema que no es posible modificar.

Archivos STAP/Z

STAP/Z proporciona archivos con datos en bruto recopilados desde DB2 (en z/OS) con sucesos DB2, sentencias SQL, etc. Este informe lista ID de interfaz, Nombre archivo UA (Suceso de auditoría sin normalizar), Nombre archivo UT (texto de suceso de auditoría sin normalizar), Nombre archivo UH (variables de host de suceso de auditoría sin

normalizar), Estado de archivo, Número tal de sucesos procesados, Número total de sucesos fallados y la Indicación de fecha y hora. Los parámetros de tiempo de ejecución son FileName Like % y FileStatus Like %.

Este informe tiene dos parámetros de tiempo de ejecución, FileName Like % y FileStatus Like %. Se basa en una consulta solo de sistema que no es posible modificar.

Excepciones de TCP

Para el periodo del informe, para cada excepción donde la Descripción de la excepción de la entidad Tipo de excepción es Excepción de protocolo TCP/IP, una fila de este informe lista los siguientes valores de atributo de la entidad Excepción: Indicación de fecha y hora de excepción, Descripción de la excepción, Dirección de origen, Dirección de destino, Puerto de origen, Puerto de destino y recuento de excepciones para dicha fila.

Tabla 64. Excepciones de TCP

Dominio	Basado en consulta	Entidad principal
Excepciones	Excepciones de TCP	Excepción
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Plantillas (CAS)

Plantillas de CAS

Este informe lista plantillas de CAS. De forma predeterminada, se listan todos los elementos de plantilla.

Tabla 65. Plantillas de CAS

Dominio	Basado en consulta	Entidad principal
Plantillas de CAS	Plantillas de CAS	Plantilla
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Access_Name	Like	%
Template_Set_Name	Like	%
Audit_Type	Like	%

Excepciones de pruebas

Indica parejas de prueba/origen de datos que están exentos temporalmente. Consulte create_test_exception para obtener más información sobre la utilización de las Excepciones de pruebas.

Tabla 66. Excepciones de pruebas

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Excepciones de pruebas	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -12 MONTH
Periodo hasta	<=	NOW

Rendimiento

Para cada Periodo de acceso en el periodo de informe, cada fila lista la hora de inicio del periodo, el recuento de direcciones IP del servidor y el número total de accesos (entidades Periodo de acceso).

Puede restringir la salida de este informe utilizando el parámetro de tiempo de ejecución de IP de servidor, que de forma predeterminada se establece en % para seleccionar todas las direcciones IP.

Tabla 67. Rendimiento

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Rendimiento del servidor de BD	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW
IP de servidor	LIKE	%

Rendimiento (gráfico)

Este informe es una versión del gráfico de Línea de etiqueta distribuida del informe de Rendimiento tabular. Representa de forma gráfica el número total de accesos del periodo del informe, un punto de datos por hora de inicio de periodo.

Puede restringir la salida de este informe utilizando el parámetro de tiempo de ejecución de IP de servidor, que de forma predeterminada se establece en % para seleccionar todas las direcciones IP.

Tabla 68. Rendimiento (gráfico)

Dominio	Basado en consulta	Entidad principal
Acceso	Rendimiento del servidor de BD - Gráfico	Periodo de acceso
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW
IP de servidor	LIKE	%

Informes de seguimiento de auditoría de actividad de usuario

El menú de Seguimiento de auditoría de actividad de usuario visualiza dos informes. Además, desde cada uno estos informes, se puede generar un tercer informe. Consulte:

- Seguimiento de auditoría de actividad de usuario
- Actividades del sistema/seguridad
- Actividad detallada de usuarios de Guardium (profundizable)

Seguimiento de auditoría de actividad de usuario

Para el periodo del informe, para cada Nombre de usuario visto en una entidad Auditoría de actividad de usuario de Guardium, cada fila visualiza el Nombre de usuario de Guardium, una Descripción de tipo de actividad (desde la entidad Tipos de activad de Guardium), un recuento de valores de entidad Modificada, el Nombre de host y el número total de entidades de Auditorías de actividad de Guardium para dicha fila.

Desde cualquier fila de este informe, el informe de Actividad detallada de usuarios de Guardium está disponible como un informe profundizable.

Tabla 69. Seguimiento de auditoría de actividad de usuario

Dominio	Basado en consulta	Entidad principal
Actividad de Guardium	Seguimiento de auditoría de actividad de usuario	Auditoría de actividad de usuario de Guardium
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Nombre de host	LIKE	%
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Actividades del sistema/seguridad

Para el periodo del informe, para cada Nombre de usuario visto en una entidad Auditoría de actividad de usuario de Guardium, cada fila visualiza el Nombre de usuario de Guardium, una Descripción de tipo de actividad (desde la entidad Tipos de activad de Guardium), un recuento de valores de entidad Modificada, el Nombre de host y el número total de entidades de Auditorías de actividad de Guardium para dicha fila.

Desde cualquier fila de este informe, el informe de Actividad detallada de usuarios de Guardium está disponible como un informe profundizable.

Tabla 70. Actividades del sistema/seguridad

Dominio	Basado en consulta	Entidad principal
Actividad de Guardium	Seguimiento de auditoría de actividad de usuario	Auditoría de actividad de usuario de Guardium
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Nombre de host	LIKE	%
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Actividad detallada de usuarios de Guardium (profundizable)

Este informe no está disponible desde el menú, pero se puede abrir desde cualquier fila en el informe Seguimiento de auditoría de actividad de usuario o desde el informe Actividades del sistema/seguridad. Para la fila seleccionada del informe, en base al Nombre de usuario y la Descripción de tipo de actividad, este informe lista los siguientes valores de atributo, que provienen de la entidad Auditoría de actividad de usuario de Guardium, excepto Descripción de tipo de actividad, que proviene de la entidad Tipos de actividad de Guardium: Nombre de usuario, Indicación de fecha y hora, Entidad Modificada, Descripción de objeto, Todos los valores y un recuento de entidades de Auditoría de actividad de usuario de Guardium.

Tabla 71. Actividad detallada de usuarios de Guardium (profundizable)

Dominio	Basado en consulta	Entidad principal
Actividad de Guardium	Actividad detallada de usuarios de Guardium	Auditoría de actividad de usuario de Guardium
Parámetro de tiempo de ejecución	Operador	Valor predeterminado

Dominio	Basado en consulta	Entidad principal
Descripción de tipo de actividad		Valor desde informe de llamada
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW
Nombre de usuario		Valor desde informe de llamada

Aviso: Los usuarios deben tener en cuenta que se registran las actividades del usuario root, y de otras cuentas de sistema confidenciales. La profundización en las actividades de estos usuarios puede mostrar mandatos y contraseñas confidenciales que se han especificado desde la línea de mandatos. Por lo tanto, los usuarios, siempre que sea posible, no deben especificar información de línea de mandatos confidencial que no les gustaría mostrar en este informe detallado.

Lista de tareas pendientes de usuario

Visualiza para cada proceso de auditoría de Guardium: una descripción, nombre de inicio de sesión, acción necesaria (revisar o aprobar), estado, usuario que ha firmado o revisado y fecha de ejecución de la tarea especificada.

Tabla 72. Lista de tareas pendientes de usuario

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Lista de tareas pendientes de usuarios	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Comentarios de usuario - Compartible

Los comentarios de usuario compartibles son todos comentarios, excepto para el motor de inspección, la política instalada y los comentarios de resultados del proceso de auditoría. Para cada comentario de usuario compartible, este informe lista los datos creados, el tipo de elemento al que se aplica (por ejemplo, a una alerta), el usuario que creó el comentario y el contenido del comentario.

Nota: Los comentarios definidos para los motores de inspección, políticas instaladas o resultados de proceso de auditoría se pueden visualizar desde las definiciones individuales, pero no se pueden visualizar en un informe.

Tabla 73. Comentarios de usuario - Compartible

Dominio	Basado en consulta	Entidad principal
Comentarios	Comentarios definidos	Comentarios
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -2 MONTH
Periodo hasta	<=	NOW

Niveles de utilización de unidad

Los siguientes informes predeterminados proporcionan datos de utilización:

- Utilización de unidad: Muestra el nivel máximo de utilización de unidad de cada unidad en el marco temporal dado. Hay un desglose que muestra detalles para una unidad en todos los periodos dentro del marco temporal del informe.
- Distribución de la utilización de la unidad: Por unidad, este informe visualiza el porcentaje de periodos en el marco temporal del informe con niveles de utilización bajo, medio y alto.
- Umbrales de utilización: Se trata de un informe predefinido que visualiza los valores de umbral altos y bajos de todos los parámetros de utilización de unidad.
- Resumen diario de utilización de la unidad: Proporciona un resumen diario de los datos de utilización de unidad.

Tabla 74. Niveles de utilización de unidad

Dominio	Basado en consulta	Entidad principal
Interno - no disponible	Distribución de utilización de unidad	Niveles de utilización de unidad
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -24 HOUR
Periodo hasta	<=	NOW

Valores modificados

Para el periodo del informe, este informe proporciona información detallada sobre los cambios de valor supervisados. Todos los valores de atributo visualizados son de la entidad Valores de supervisor. La consulta en la que se basa este informe tiene una secuencia de clasificación no estándar, como se indica a continuación:

- IP de servidor
- Tipo de BD
- Indicación de fecha y hora de auditoría
- Nombre de tabla de auditoría
- Propietario de auditoría

La consulta en la que se basa este informe tiene varios parámetros de tiempo de ejecución, todos los cuales utilizan el operador LIKE con el valor predeterminado de %, lo que significa que se seleccionarán todos los valores.

Para cada valor supervisado seleccionado, una fila del informa lista la Indicación de fecha y hora, IP de servidor, Tipo de BD, Nombre de servicio, Nombre de base de datos, Nombre inicio sesión auditoría, Indicación de fecha y hora de auditoría, Nombre de tabla de auditoría, Propietario de auditoría, Acción de auditoría, Valor anterior de auditoría, Valor nuevo de auditoría, Texto SQL, ID desencadenado y un recuento de las entidades Columnas cambiadas para dicha fila.

Tabla 75. Valores modificados

Dominio	Basado en consulta	Entidad principal
Valor modificado	Valores modificados	Columnas cambiadas
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Acción de auditoría	LIKE	%
Nombre de inicio de sesión de auditoría	LIKE	%
Propietario de auditoría	LIKE	%
Nombre de tabla de auditoría	LIKE	%
Tipo de BD	LIKE	%
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW
IP de servidor	LIKE	%

Tema principal: Cómo sacar provecho de los informes predefinidos

Informes de usuario predefinidos

Esta sección proporciona una descripción breve de todos los informes predefinidos en el diseño de usuario predeterminado.

Para obtener una descripción de los informes sobre el diseño de administrador predeterminado, consulte Informes de administrador predefinidos.

Nota: Si se ha habilitado la seguridad a nivel de datos observados (consulte valores de Perfil global), entonces se filtrará la salida del proceso de auditoría para que los usuarios sólo vean la información de sus bases de datos.

Ver política instalada

El informe Política actualmente instalada muestra información sobre la política instalada. Pulse el enlace de política instalada para visualizar las reglas de política en una ventana aparte.

Número de bd por tipo

Muestra el número de servidores y clientes para cada tipo de base de datos supervisada (el periodo de tiempo predeterminado es el día actual).

Velocidad de solicitudes

De forma predeterminada, muestra la velocidad de las solicitudes durante las últimas dos horas. Este informe gráfico está pensado para visualizar solo la actividad reciente. Si modifica los parámetros de tiempo de ejecución Desde y Hasta para incluir un marco temporal mayor, es posible que reciba un mensaje que indica que hay demasiados datos. (Utilice un informe tabular para mostrar un periodo de tiempo mayor).

Sesiones por tipo de servidor

Para cada tipo de servidor (DB2, Informix, etc.), una fila de este informe muestra el número total de sesiones que se han abierto durante el periodo de informe (de forma predeterminada, las tres últimas horas).

Ejecución de DML en objetos confidenciales

Para cada Verbo SQL del grupo de Mandatos DML que hace referencia a un Nombre de objeto del grupo Objetos confidenciales, este informe muestra una fila para cada Periodo de acceso, IP de cliente y Programa fuente, con un recuento total de objetos referenciados en dicha fila. Aunque el título del informe contiene la palabra Ejecuciones, no hay ninguna garantía de que se hayan ejecutado realmente todos los mandatos.

Uso de objetos confidenciales

Para cada objeto del grupo Objetos confidenciales, muestra una fila por cada IP de cliente y Programa fuente que hace referencia al objeto durante el periodo de informe, y un recuento de referencias de objeto.

El grupo Objetos confidenciales está vacío en el momento de la instalación. Alguien de su empresa debe rellenar el grupo con el conjunto de miembros adecuado.

Actividad por IP de cliente

Para cada dirección IP de cliente vista durante el periodo de informe, una fila cuenta el número de Verbos de SQL, Nombres de objeto y el número total de sesiones.

Servidores de base de datos

Para cada dirección IP de servidor a la que se accede durante el periodo de informe, una fila del informe muestra el Tipo de servidor, el Nombre de base de datos, el Nombre de servicio, un recuento de los programas fuente que acceden a ese servidor y el número total de sesiones para dicha fila.

Acceso a IMS (z/OS)

Utilícelo para notificar el acceso a IMS (z/OS).

Tabla 1. Acceso a IMS (z/OS)

Dominio	Basado en consulta	Entidad principal
Acceso	Acceso a IMS	Cliente Servidor
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -2 HOUR
Periodo hasta	<=	NOW

Objeto de IMS (z/OS)

Utilícelo para notificar el objeto para IMS (z/OS).

Tabla 2. Objeto de IMS (z/OS)

Dominio	Basado en consulta	Entidad principal
Acceso	Objeto IMS	Objeto
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -2 HOUR
Periodo hasta	<=	NOW

Suceso de IMS (z/OS)

Utilícelo para notificar el suceso a IMS (z/OS).

Tabla 3. Suceso de IMS (z/OS)

Dominio	Basado en consulta	Entidad principal
Acceso	Suceso de IMS	SQL
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -2 HOUR
Periodo hasta	<=	NOW

Detalles de acceso a datos de IMS (z/OS)

Utilícelo para notificar los detalles de acceso a datos a IMS (z/OS).

Tabla 4. Detalles de acceso a datos de IMS (z/OS)

Dominio	Basado en consulta	Entidad principal
Acceso	Detalles de acceso a datos de IMS	SQL completo
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -2 HOUR
Periodo hasta	<=	NOW
IP de cliente	LIKE	
DBUserName	LIKE	
Nombre de IMS	LIKE	
ServerIP	LIKE	

Infracciones de política

Para cada infracción de reglas de política registrada durante el periodo de creación de informes, este informe proporciona la Indicación de fecha y hora de la entidad Infracción de reglas de política, Descripción de regla de acceso, IP de cliente, IP de servidor, Nombre de usuario de BD, Serie SQL completo de la entidad Infracción de reglas de política, Descripción de la gravedad y un recuento de infracciones para dicha fila. No puede acceder a la consulta en la que se basa este informe (Lista de infracciones de política con gravedad), pero puede clonar el informe.

Distribución de excepciones

Cada porción del diagrama circular representa la proporción de excepciones para cada valor de atributo de Descripción de excepción (de la entidad Tipo de excepción) que se ha registrado durante el periodo del informe.

Al igual que con cualquier gráfico, puede detallar más en el gráfico circular para mostrar la versión tabular de la consulta en la que se basa el gráfico. Hay varios informes de excepciones a los que se puede acceder desde este informe tabular (o detalles de la misma) que están disponibles aquí, pero que no están incluidos en ningún menú.

Supervisor de excepciones

Un recuento de excepciones registradas durante el periodo del informe. Se crea un punto de datos cada vez que se renueva el informe en el portal.

Intentos de inicio de sesión de usuario fallidos

Para cada intento de inicio de sesión fallido durante el periodo de informe, lista el Nombre de usuario, la Dirección de origen, la Dirección de destino y el Tipo de protocolo de base de datos para el servidor en el que el usuario estaba intentando iniciar la sesión.

Errores de SQL

Para cada error de SQL durante el periodo del informe, muestra la dirección IP del cliente, la dirección IP del servidor, el Tipo de servidor, el nombre de usuario de la base de datos, el texto de error de la base de datos y el total de apariciones de errores para dicho registro.

Recuento de excepciones

El número total de excepciones (Entidades de excepción) registradas durante el periodo del informe.

Inicios de sesión de usuarios finalizados

Lista todos los inicios de sesión por usuarios de base de datos que son miembros del grupo Usuario de BD terminado. Cada fila lista un Nombre de usuario de BD, IP de cliente, IP de servidor, Tipo de servidor, Programa fuente, hora del último inicio de sesión (el valor máximo del atributo Inicio de sesión) y el recuento de sesiones para la fila.

El grupo Usuarios de BD terminados está vacío en el momento de la instalación. Debe ser rellenado por alguien en su ubicación. No se puede acceder a la consulta en la que se basa este informe (Inicios de sesión de usuarios terminados) desde ningún creador de consultas.

Último inicio de sesión de usuarios activos

Último inicio de sesión registrado durante el periodo de creación de informes para cada miembro del grupo Usuarios activos. Se listarán todos los miembros del grupo, incluso si no habían inicios de sesión durante el periodo de informe. Esto es distinto a la mayoría de los informes basados en miembros de un grupo. En el caso "normal", si no se encuentra ninguna actividad para un miembro, ese miembro no aparece en la lista.

Cada fila lista un Nombre de usuario de BD, IP de cliente, IP de servidor, Tipo de servidor, Programa fuente, hora del último inicio de sesión (el valor máximo del atributo Inicio de sesión) y el recuento de sesiones para la fila.

El grupo Usuarios activos está vacío en el momento de la instalación. Debe ser rellenado por alguien en su ubicación. No se puede acceder a la consulta en la que se basa este informe (Últimos inicios de sesión de usuarios activos) desde ningún creador de consultas.

Usuarios activos sin actividad

Listado de los miembros del grupo Usuarios activos que no han tenido ninguna actividad durante el periodo del informe. Este informe estará vacío si todos los usuarios han tenido actividad durante el periodo del informe.

El grupo Usuarios activos está predefinido, pero está vacío en el momento de la instalación. Debe ser rellenado por alguien en su ubicación. No se puede acceder a la consulta en la que se basa este informe (Usuarios activos sin actividad) desde ningún creador de consultas.

Intentos de inicio de sesión fallidos de los usuarios finalizados

Lista los intentos fallidos de inicio de sesión por usuarios de base de datos que son miembros del grupo Usuario de BD terminado. Este informe estará vacío si no hubo intentos de inicio de sesión fallidos por parte de nadie de este grupo durante el periodo del informe.

El grupo Usuarios de BD terminados está predefinido, pero está vacío en el momento de la instalación. Debe ser rellenado por alguien en su ubicación. No se puede acceder a la consulta incorporada para este informe. No se puede acceder a la consulta en la que se basa este informe (Intentos de inicio de sesión fallidos de usuarios terminados) desde ningún creador de consultas.

Errores excesivos por periodo

Visualice números de errores/periodo; p. ej., más de N errores en 60 min para la misma dirección IP de cliente, dirección IP de servidor, Tipo de servidor, Nombre de usuario de base de datos.

Usuarios inactivos desde

Mostrar Último inicio de sesión e Inicio de sesión del usuario para todos los usuarios que tienen Registros de acceso y que tienen un tiempo de Inicio de sesión máximo anterior a 90 días. (Se pierde un usuario inactivo si nunca han iniciado la sesión, o si se han depurado todos los inicios de sesión antiguos)

Inicio de sesión de usuarios de administración

Para cada Nombre de usuario de BD incluido en el grupo Usuarios de administración, que tenían una o más sesiones durante el periodo de informe, cada fila lista la IP de cliente, el Nombre de usuario de BD, el Programa fuente, la Hora de inicio de sesión y el Recuento de sesiones para dicha fila.

Inicio de sesión de los usuarios predefinidos de la BD

Para cada Nombre de usuario de BD incluido en el grupo Usuarios predefinidos de BD, que tenían una o más sesiones durante el periodo de informe, cada fila lista el Nombre de usuario de BD, IP de cliente, IP de servidor, Programa fuente, Nombre de base de datos, Nombre de servicio y Recuento de sesiones para dicha fila.

Uso de mandatos administrativos

Para cada Verbo SQL incluido en el grupo Mandatos administrativos que se ha visto durante el periodo del informe, este informe lista el Verbo SQL, Profundidad, Nombre de objeto e IP de cliente y un recuento de objetos referenciados.

Uso de objetos administrativos

Para cada Nombre de objeto incluido en el grupo Objetos de administración que se ha visto durante el periodo de informe, cada fila lista el Nombre de objeto, IP de cliente, IP de servidor, Nombre de servicio, Nombre de base de datos, Programa fuente, Nombre de usuario de BD y Recuento de objetos para dicha fila.

Ejecución de DML en objetos de administración

Para cada Verbo SQL del grupo Mandatos DML que hace referencia a un Nombre de objeto del grupo Objetos de administración, este informe muestra una fila para el Nombre de usuario de BD, IP de cliente, IP de servidor, Tipo de servidor, Nombre de servicio, Nombre de base de datos, Verbo SQL, Nombre de objeto y Recuento de objetos a los que se hace referencia en la fila.

Ejecución de mandatos BACKUP

Para cada Verbo SQL del grupo de Mandatos BACKUP visto durante el periodo de informe, este informe muestra la IP de cliente, IP de servidor, Nombre de servicio, Nombre de usuario de BD, Programa fuente, Nombre de base de datos, Nombre de objeto, Verbo SQL y Recuento de objetos referenciados en la fila.

Ejecución de mandatos RESTORE

Para cada Verbo SQL del grupo de Mandatos BACKUP visto durante el periodo de informe, este informe muestra la IP de cliente, IP de servidor, Nombre de servicio, Nombre de usuario de BD, Programa fuente, Nombre de base de datos, Nombre de objeto, Verbo SQL y Recuento de objetos referenciados en la fila.

Ejecución de mandatos REVOKE

Para cada Verbo SQL del grupo de Mandatos REVOKE visto durante el periodo de informe, este informe muestra la IP de cliente, IP de servidor, Nombre de servicio, Nombre de usuario de BD, Programa fuente, Nombre de base de datos, Nombre de objeto, Verbo SQL y Recuento de objetos a los que se hace referencia en la fila.

Ejecución de mandatos KILL

Para cada Verbo SQL del grupo de Mandatos KILL visto durante el periodo de informe, este informe muestra la IP de cliente, IP de servidor, Nombre de servicio, Nombre de usuario de BD, Programa fuente, Nombre de base de datos, Nombre de objeto, Verbo SQL y Recuento de objetos a los que se hace referencia en la fila.

Ejecución de mandatos DBCC

Para cada Verbo SQL del grupo de Mandatos DBCC visto durante el periodo de informe, este informe muestra la IP de cliente, IP de servidor, Nombre de servicio, Nombre de usuario de BD, Programa fuente, Nombre de base de datos, Sentencia SQL y Recuento de objetos a los que se hace referencia en la fila.

Ejecución de mandatos GRANT

Para cada Verbo SQL del grupo de Mandatos GRANT visto durante el periodo de informe, este informe muestra la IP de cliente, IP de servidor, Nombre de servicio, Nombre de usuario de BD, Programa fuente, Nombre de base de datos, Nombre de objeto, Verbo SQL y Recuento de objetos a los que se hace referencia en la fila.

Utilización de cuenta con privilegios

Muestra el Usuario, el Verbo y el Recuento de Periodos dentro de los que un Usuario ha realizado el Verbo en el grupo Usuarios de administración

Acceso del usuario con privilegios de objetos de negocio

Muestra el Usuario, el Verbo y el Objeto donde se ha realizado el Usuario de Usuarios de administración y el Verbo en un Objeto que se encuentra en un grupo seleccionado de Objetos de negocio

Ejecución de mandatos CREATE

Para cada Verbo SQL del grupo Mandatos CREATE vistos durante el periodo de informe, este informe muestra la IP de cliente, IP de servidor, Nombre de servicio, Nombre de usuario de BD, Programa fuente, Nombre de base de datos, Nombre de objeto, Verbo SQL y Recuento de objetos referenciados en la fila.

Mandatos DDL

Todos los mandatos DDL enviados a la base de datos. El informe muestra la IP del cliente desde la que se ha solicitado el DDL, el verbo SQL principal (un mandato DDL específico) y el total de objetos a los que se ha accedido para dicho registro.

Para cada Verbo SQL del grupo de Mandatos DDL visto durante el periodo de informe, este informe muestra la IP de cliente, IP de servidor, Tipo de servidor, Verbo SQL y Recuento de mandatos referenciados en la fila.

Ejecución de mandatos ALTER

Se han emitido todos los mandatos ALTER. El informe muestra la IP de cliente desde la que se ha solicitado el DDL, la dirección IP del servidor, el nombre de servicio, el nombre de usuario de base de datos, el programa fuente, el nombre de base de datos, el nombre de objeto y el verbo SQL principal (un mandato DDL específico) para cada combinación de mandato IP/DDL de cliente listada en esa línea específica.

Para cada Verbo SQL del grupo Mandatos ALTER visto durante el periodo de informe, este informe muestra la IP de cliente, IP de servidor, Nombre de servicio, Nombre de usuario de BD, Programa fuente, Nombre de base de datos, Nombre de objeto, Verbo SQL y Recuento de objetos a los que se hace referencia en la fila.

Distribución de DDL

Este gráfico de barras visualiza la distribución de mandatos vistos desde el grupo Mandatos DDL durante el periodo de informe. Para cada mandato visto, una sola barra representa el número total de objetos afectados.

Ejecución de mandatos DROP

Para cada Verbo SQL del grupo Mandatos DROP visto durante el periodo de informe, este informe muestra la IP de cliente, IP de servidor, Nombre de servicio, Nombre de usuario de BD, Programa de origen, Nombre de base de datos, Nombre de objeto, Verbo SQL y Recuento de objetos a los que se hace referencia en la fila.

Un usuario una IP

Para cada Nombre de usuario de BD para el que se han recopilado datos durante el periodo de informe, cada línea de este informe muestra el recuento de direcciones IP de cliente desde las que el usuario ha iniciado la sesión y un número total de sesiones.

Resumen de actividad del IP del cliente

Este informe visualiza la actividad del periodo de informe desde una única dirección IP de cliente, que se especifica como un parámetro de tiempo de ejecución. Cada fila del informe muestra la IP de cliente, el Programa de origen, el Verbo SQL, la Profundidad (de la frase dentro del mandato SQL), un Nombre de objeto y un recuento de veces que se ha hecho referencia a ese objeto para dicha fila.

Lista de sesiones

Este informe lista todas las sesiones de base de datos para el periodo de informe. Para cada sesión, el informe muestra la Indicación de fecha y hora de la sesión (entidad), Inicio de sesión (indicación de fecha y hora), Tipo de servidor, IP de cliente, IP de servidor, Puerto de cliente, Puerto de servidor, Protocolo de red, Protocolo de BD, Versión de protocolo de BD, Nombre de usuario de BD, Programa de origen y Recuento de sesiones para dicha fila (que siempre debe ser 1).

Al igual que con la mayoría de los informes, están disponibles los informes detallados. Hay una serie de informes de sesión a los que se puede acceder desde este informe, pero que no están incluidos en ningún menú. Esto incluye los informes siguientes, con los parámetros de tiempo de ejecución para ese conjunto de informes utilizando valores de la fila seleccionada del informe:

Tabla 5. Lista de sesiones

Informe	Parámetros de tiempo de ejecución
Sesiones por IP de cliente	IP de servidor, Tipo de servidor
Sesiones por IP de servidor	Tipo de servidor
Sesiones por programa fuente	Tipo de servidor, IP de servidor
Sesiones por usuario	Tipo de servidor, IP de servidor
Detalles de sesiones por servidor	Tipo de servidor, IP de servidor

Lista de mandatos

Este informe lista todos los Verbos SQL vistos durante el periodo de informe. En el nivel más externo, los mandatos se agrupan por la hora de Inicio del periodo desde la entidad Periodo de acceso, que normalmente es una hora, a la hora. El administrador de Guardium puede modificar la longitud del periodo de acceso cambiando la granularidad de registro, que es una hora de forma predeterminada. Para cada Periodo de informe del periodo de creación de informes, cada fila lista la hora de Inicio del periodo de acceso, un Verbo SQL, la Profundidad del verbo en la sentencia SQL, el Padre (un puntero al verbo propietario) y un recuento de apariciones para la fila.

Lista de objetos

Este informe lista todos los objetos vistos durante el periodo de informe. En el nivel más externo, los objetos se agrupan por la hora de Inicio del periodo desde la entidad Periodo de acceso, que normalmente es una hora, a la hora. El administrador de Guard de SQL puede modificar la longitud del periodo de acceso cambiando la granularidad del registro, que es una hora de forma predeterminada. Para cada Periodo de acceso en el periodo de informe, cada fila lista la hora de Inicio del periodo de acceso, un Nombre de objeto y el recuento de apariciones de dicha fila.

Resumen de actividad de objetos

Este informe muestra la actividad de periodo de informe para un único Nombre de objeto, que se especifica como un parámetro de tiempo de ejecución. Cada fila del informe muestra la IP de cliente, el Programa de origen, el Verbo SQL, la Profundidad (de la frase dentro del mandato SQL), un Nombre de objeto y un recuento de veces que se ha hecho referencia a ese objeto para dicha fila.

Candidatos de archivado

Este informe lista objetos (tablas de base de datos o procedimientos almacenados, por ejemplo) a los que no se ha accedido durante un periodo de tiempo ampliado. No puede acceder a la consulta en la que se basa este informe.

Actividad de compartición de archivos de Windows

Este informe lista toda la actividad de SQL de Compartición de archivos de Windows que se ha visto durante el periodo de creación de informes. En el nivel más externo, los mandatos SQL se agrupan por la hora de Inicio del periodo desde la entidad Periodo de acceso, que normalmente es una hora, a la hora. El administrador de Guardium puede modificar la longitud del periodo de acceso cambiando la granularidad de registro, que es una hora de forma predeterminada. Para cada Periodo de acceso del periodo de creación de informes, cada fila lista la hora de Inicio del periodo de acceso, el Nombre del servicio, la IP del cliente, la IP del servidor, el Programa fuente, SQL (de la entidad SQL) y un recuento de apariciones para la fila. No puede acceder a la consulta en la que se basa este informe, pero puede clonar el informe.

Detalles del acceso por horas

Este informe produce una lista muy detallada para cada Nombre de usuario de BD visto en el periodo de informe, que es una hora de forma predeterminada para este informe. Cada fila del informe lista un Nombre de usuario de BD, IP de cliente, IP de servidor, Inicio de periodo, Programa fuente, SQL (de la entidad de SQL) y un recuento de apariciones durante el periodo de acceso.

SQL completo por nombre de usuario de BD

Este informe muestra los valores de atributo de SQL completo del periodo de informe que se han registrado para un único Nombre de usuario de BD, que se especifica como un parámetro de tiempo de ejecución. Cada fila del informe muestra el ID de SQL completo, la Indicación de fecha y hora (de la entidad de SQL completo), la IP de cliente, el Nombre de usuario de BD, el Inicio de sesión, el Programa fuente, SQL completo y un recuento de las apariciones de la fila.

SQL completo por ID de cliente

Este informe muestra los valores de atributos de SQL completo de periodo de informe que se han registrado para una IP de cliente individual, que se especifica como un parámetro de tiempo de ejecución. Cada fila del informe muestra el ID de SQL completo, la Indicación de fecha y hora (de la entidad de SQL completo), la IP de cliente, el Nombre de usuario de BD, el Inicio de sesión, el Programa fuente, SQL completo y un recuento de las apariciones de la fila.

Lista de Flat LOG

Lista las tareas de proceso de flat log.

Resultados del proceso de clasificación

Lista las tareas del proceso de clasificación.

Objetos latentes de DW

Muestra todos los miembros de un grupo que no son miembros de un segundo grupo, con un foco en tablas latentes. Por ejemplo, este informe muestra los objetos que se encuentran en el grupo Todos los objetos, pero que no se han utilizado en una Selección.

Objetos/campos latentes de DW

Muestra todos los miembros de un grupo que no son miembros de un segundo grupo, con un foco en las columnas y tablas latentes. En esta instancia, los grupos son un tipo de 2 tuplas (miembros que son un compuesto de un par de atributos de valor). Por ejemplo, este informe muestra los objetos que están en el grupo Todos los objetos y campos, pero que no se han utilizado en una Selección.

Acceso a objetos de DW EXECUTE

Utilice este informe para llenar el grupo denominado Objetos de DW EXECUTE con un conjunto de nombres de procedimientos almacenados que se está ejecutando. A continuación, utilice la correlación indirecta de Creador de grupos/Proxy de llamada generado automáticamente para generar todos los objetos que se utilizan en estos procedimientos.

Acceso a objetos de DW SELECT

Este informe muestra todos los nombres de objetos a los que se ha accedido mediante una sentencia SELECT.

Acceso de objeto-campo de DW SELECT

Este informe muestra todos los nombres de objeto y campo a los que se ha accedido mediante una sentencia SELECT.

Consultas de larga ejecución

Para el periodo de creación de informes, este informe lista las consultas de ejecución más largas, con el tiempo medio de ejecución más largo primero. Para cada consulta, lista la IP de cliente, IP de servidor, SQL, Inicio de periodo (desde la entidad Periodo de acceso), Tiempo promedio de ejecución y el recuento de apariciones de esta fila. No puede acceder a la consulta en la que se basa este informe.

Rendimiento

Este informe genera un recuento de todas las IP de servidor vistas, y de todos los accesos, durante el periodo de informe. En el nivel más externo, los accesos se agrupan por la hora de Inicio del periodo desde la entidad Periodo de acceso, que normalmente es una hora, a la hora. El administrador de Guardium puede modificar la longitud del periodo de acceso cambiando la granularidad de registro, que es una hora de forma predeterminada. Cada fila lista la hora de Inicio del periodo, el recuento de las IP de servidor vistas y un recuento total de accesos para la fila.

Puede restringir la salida de este informe utilizando el parámetro de tiempo de ejecución de IP de servidor, que de forma predeterminada se establece en “%” para seleccionar todas las direcciones IP.

Rendimiento (gráfico)

Este informe es una versión del diagrama de Línea de etiqueta distribuida del informe Rendimiento tabular, trazando el número total de accesos durante el periodo de informe, un punto de datos por hora de Inicio de periodo.

Puede restringir la salida de este informe utilizando el parámetro de tiempo de ejecución de IP de servidor, que de forma predeterminada se establece en “%” para seleccionar todas las direcciones IP.

Número de tareas del conjunto de privacidad activas

Número de procesos de auditoría de Guardium activos que contienen una o más tareas de conjunto de privacidad. Cuando se utiliza la gestión central, este informe sólo contiene datos sobre el Gestor central y está vacío en todas las unidades gestionadas (aparece el mensaje estándar No se han encontrado datos para la consulta solicitada). Este informe tiene parámetros de tiempo de ejecución no estándares: no hay parámetros de fecha desde y hasta, por lo que se informará de todos los procesos de auditoría que contengan una o varias tareas de conjunto de privacidad. Puede clonar la consulta en la que se basa este informe (Número de procesos de conjunto de privacidad activos), pero no puede clonar ni volver a generar el informe predeterminado. La consulta clonada tendrá todos los parámetros de tiempo de ejecución estándar (incluidas las fechas desde y hasta).

Cola de trabajos de Guardium

Muestra la cola de trabajos de Guardium. Para cada trabajo, lista el ID de ejecución del proceso, Tipo de proceso, Estado, ID de proceso de Cls/Asmt, ID de resultado de informe, Descripción de Cls/Asmt, Descripción de tarea de auditoría, Tiempo de cola, Hora de inicio, Hora de finalización, y Orígenes de datos.

Tabla 6. Cola de trabajos de Guardium

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Cola de trabajos de Guardium	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Descripción de trabajo	LIKE	%
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Bases de datos descubiertas

Para el periodo de informe, para cada entidad Puerto descubierto donde el valor de atributo Tipo de BD es NOT LIKE Desconocido, este informe lista la Indicación de fecha y hora de sondeo, IP de servidor, Nombre de host de servidor, Tipo de BD, Puerto, Tipo de puerto y un recuento de Puertos descubiertos por fila.

Tabla 7. Bases de datos descubiertas

Dominio	Basado en consulta	Entidad principal
Descubrimiento automático	Bases de datos descubiertas	Puerto descubierto
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Orígenes de datos

Este informe aparece en el diseño predeterminado tanto para los administradores como para los usuarios. Consulte Orígenes de datos en la página Informes predefinidos - Común.

Historial de versiones de origen de datos

Este informe aparece en el diseño predeterminado tanto para los administradores como para los usuarios. Consulte Historial de versiones de origen de datos en la página Informes predefinidos - Común.

Cola de trabajos de Guardium

Muestra la cola de trabajos de Guardium. Para cada trabajo, lista el ID de ejecución del proceso, Tipo de proceso, Estado, ID de proceso de Cls/Asmt, ID de resultado de informe, Descripción de Cls/Asmt, Descripción de tarea de auditoría, Tiempo de cola, Hora de inicio, Hora de finalización, y Orígenes de datos.

Revisiones del proceso de auditoría pendientes

Para cada Nombre de inicio de sesión de usuario de Guardium, este informe lista el número y el tipo de procesos de auditoría de Guardium pendientes. Un proceso de auditoría pendiente tiene un valor de atributo de Estado (en la entidad Lista de tareas pendientes de resultados de tarea) que no sea Revisado o Firmado. Este informe tiene parámetros de tiempo de ejecución no estándar: no hay fechas desde ni hasta, lo que significa que se notificarán todos los resultados de tareas pendientes. Puede clonar la consulta en la que se basa este informe (tiene el mismo nombre), pero no puede clonar ni volver a generar el informe predeterminado. La consulta clonada tendrá todos los parámetros de tiempo de ejecución estándar (incluidas las fechas desde y hasta).

Número de procesos de auditoría activos

El número de procesos de auditoría de Guardium activos. Cuando se utiliza la gestión central, este informe sólo contiene datos sobre el Gestor central y está vacío en todas las unidades gestionadas (aparece el mensaje estándar No se han encontrado datos para la consulta solicitada). Este informe tiene parámetros de tiempo de ejecución no estándar: no hay ningún parámetro de fecha desde y hasta, por lo que se notificarán todos los procesos de auditoría. Puede clonar la consulta en la que se basa este informe (Número de procesos activos), pero no puede clonar ni volver a generar el informe predeterminado. La consulta clonada tendrá todos los parámetros de tiempo de ejecución estándar (incluidas las fechas desde y hasta).

Ver política instalada

En el panel Política instalada actualmente, este informe especial visualiza la información sobre la política instalada como, por ejemplo, el nombre de la política, el número de reglas que contiene y los valores de definición de política. No puede acceder a la consulta en la que se basa este informe.

Recuento de infracciones de política

Para el periodo de creación de informes, este informe muestra el número de infracciones de política registradas.

Alertas de umbral registradas

Este informe muestra una barra que representa el número total de alertas registradas durante el periodo del informe, para cada tipo de alerta de umbral registrado, en función del atributo Descripción de la alerta de la entidad Detalles de alerta de umbral.

Alertas en tiempo real registradas

Este informe visualiza una barra que representa el número total de alertas registradas durante el periodo de informe, para cada tipo de alerta en tiempo real registrada, basada en el atributo Descripción de la regla de acceso de la entidad Infracción de reglas de política.

Infracciones/Incidencias

Consulte el tema Gestión de incidencias.

Tema principal: Cómo sacar provecho de los informes predefinidos

Común de informes predefinidos

En esta sección se proporciona una breve descripción de todos los informes predefinidos en los diseños de usuario predeterminado y de administrador predeterminado.

Los informes comunes son:

- Historial de versiones de origen de datos
- Orígenes de datos

Supervisor de estado

El informe gráfico del Supervisor de estado muestra el estado actual del dispositivo Guardium: cuántos paquetes por segundo y solicitudes por segundo se procesan, la cantidad de espacio de disco y de memoria que se está utilizando, y así sucesivamente. Cada campo se describe en la tabla siguiente.

El recuadro muestra la salida del mandato VMSTAT de Linux. Si está familiarizado con este mandato, estas estadísticas deben resultarle familiares.

Tabla 1. Supervisor de estado

Campo	Descripción
procesos	El número de procesos: **r**: En espera del tiempo de ejecución. **b**: En suspensión ininterrumpible (bloqueada, a la espera de otro suceso).
memoria	Uso de memoria (kB): **swpd**: Cantidad de memoria virtual utilizada. **free**: Cantidad de memoria desocupada. **buff**: Cantidad utilizada como almacenamientos intermedios. **cache**: Cantidad reservada para la memoria caché.
intercambio	Cantidad de memoria (kB): **si**: Se intercambia desde el disco. **so**: Se intercambia hacia el disco.
e/s	Bloques de entrada/salida (kB/s): **bi**: Bloques recibidos de un dispositivo de bloque **bo**: Bloques enviados a un dispositivo de bloque
sistema	Sistema: **in**: Interrupciones por segundo, incluido el reloj **cs**: Conmutadores de contexto por segundo
cpu	Porcentaje del tiempo total de CPU utilizado por: **us**: Tiempo dedicado a la ejecución de código no de kernel **sy**: Tiempo dedicado a la ejecución de código de kernel **id**: Tiempo de inactividad (sin incluir espera de E/S) **wa**: Tiempo dedicado a la espera de E/S **st**: Tiempo robado de una máquina virtual
(n)pps / (m)rps	En la flecha situada junto al Motor de análisis, se calculan dos promedios para los últimos cinco segundos: **n** es el número medio de paquetes de red por segundo, y **m** es el número medio de solicitudes de base de datos de red por segundo.
Motor de análisis (q-d) ------ (p)	Para el Motor de análisis, la primera línea lista el número total de mensajes en cola para su proceso (**q**), seguidos por el número de mensajes descartados (**d**) porque el almacenamiento intermedio estaba en peligro de llenarse. La segunda línea lista el número total de mensajes procesados (**p**). El número procesado se restablecerá a cero siempre que se reinicie el motor de inspección.
Tipo de servidor (q) ---- (p)	Para cada tipo de servidor, se lista el número de mensajes que esperan proceso (**q**) y se lista el número de mensajes procesados (**p**).
Espacio libre en disco	El número de bytes libres.
n% de BD lleno	El porcentaje de la asignación de espacio de base de datos que se utiliza.

Campo	Descripción
Archivos/Otros	La parte Archivos/Otros del Supervisor de estado representa los datos acumulados en el registrador nondb-sql. El registrador nondb-sql registra los sucesos de sesión de cierre que llegan al Analizador desde sesiones “ignoradas” que el Analizador ha cerrado internamente (INACTIVE_FLAG=-1). El Analizador tiene la capacidad de cerrar conexiones por tiempo de espera (si la sesión ha estado inactiva durante mucho tiempo). Si los datos de sesión de cierre llegan al Analizador desde la sesión "ignorada" que ha sido cerrada por el tiempo de espera, se registrará en la sección nondb-sql-logger. El Analizador nunca registra los datos directamente en la base de datos. Esta sección también representa el número de solicitudes BD (como las inserciones en GDM_SECURE_PARAMS) enviadas por el Analizador al Registrador, así como otros protocolos soportados como, por ejemplo, FTP

Historial de versiones de origen de datos

Ubicación de diseño predeterminado

- admin: disponible como profundización desde el informe Orígenes de datos
- user: Descubrir > Descubrimiento de BD

Orígenes de datos

Lista todos los orígenes de datos definidos: Tipo de origen de datos, Nombre de origen de datos, Descripción de origen de datos, Host, Puerto, Nombre de servicio, Nombre de usuario, Nombre de base de datos, Última conexión, Compartido y Propiedades de conexión.

Puede restringir la salida de este informe utilizando el parámetro de tiempo de ejecución Nombre de origen de datos, que, de forma predeterminada, se establece en "%" para seleccionar todos los orígenes de datos.

Tabla 2. Orígenes de datos

Dominio	Basado en consulta	Entidad principal
interno - no disponible	Orígenes de datos	no disponible
Parámetro de tiempo de ejecución	Operador	Valor predeterminado
Nombre de origen de datos	LIKE	%
Periodo desde	>=	NOW -1 DAY
Periodo hasta	<=	NOW

Procesos de auditoría predefinidos

Existe un proceso de auditoría predefinido denominado Supervisión de dispositivos, que contiene los informes siguientes. Este proceso de auditoría está inactivo de forma predeterminada. El administrador puede activarlo y planificarlo según sus necesidades.

Nota: Cuando planifique este proceso de auditoría, compruebe que las fechas DESDE/HASTA de cada informe tienen sentido para el intervalo de proceso que se define (por ejemplo, no tiene sentido tener un periodo de informe de un día si el proceso de auditoría se ejecuta sólo una vez a la semana: se perderán seis días de actividad). El proceso de auditoría de Supervisión de dispositivos contiene los informes siguientes:

- Inicios de sesión fallidos en Guardium
- Usuarios activos de Guardium
- Errores de agregación/archivado
- Cambios relacionados con la política
- Motores de inspección y cambios de S-TAP
- Cambios en el origen de datos
- Cambios en la configuración de instancia de CAS
- Instancias de CAS
- Plantillas de CAS
- Excepciones de trabajos planificados

Tema principal: Cómo sacar provecho de los informes predefinidos

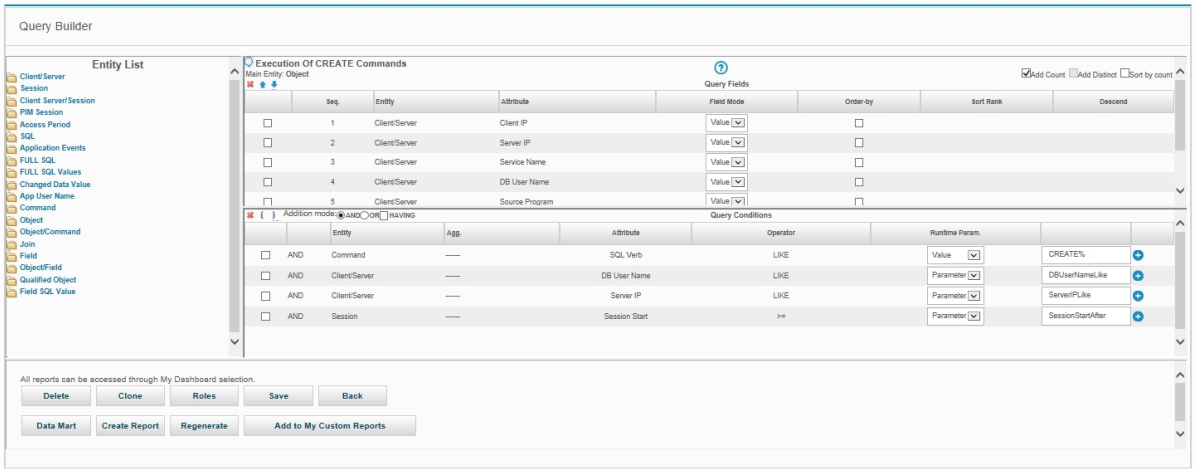
Cómo formular preguntas de los datos

Utilice el Creador de consultas para definir y modificar preguntas sobre los datos recopilados.

Hay una distinción entre consultas e informes:

- Una consulta describe un conjunto de información que se debe obtener de los datos recopilados; por ejemplo, buscar todos los clientes que actualizan una base de datos específica durante las horas de fin de semana o qué usuarios no autorizados han intentado acceder a datos confidenciales (números de Seguridad Social o número de tarjeta de crédito).
- Un informe describe cómo se presentan los datos devueltos por una consulta.

Existe un Creador de consultas independiente para cada dominio, y se abre desde el Buscador de consultas para ese dominio (consulte la sección Abrir el buscador de consultas). Pulse Informes > Herramientas de configuración de informes > Creador consultas.



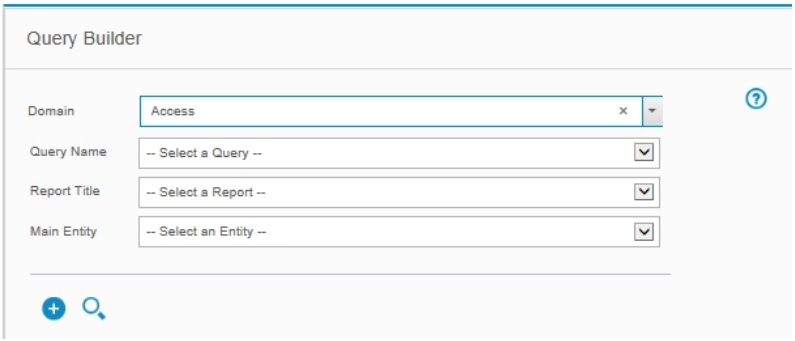
El creador de consultas contiene tres paneles:

- El panel Lista de entidades identifica todas las entidades y atributos que están contenidos en el dominio. Las entidades se representan como carpetas, y los atributos son los elementos que hay dentro. Pulse una carpeta de entidad para mostrar sus atributos, o pulse otra vez para ocultarlos. Para obtener una descripción de todas las entidades y atributos, consulte Entidades y atributos en el tema de ayuda Dominios, entidades y atributos.
- El panel Campo de consulta lista todos los campos a los que se debe acceder, lo que se debe visualizar para ese campo (su valor, un recuento, mínimo, máximo o promedio) y el orden de clasificación. Para obtener más información sobre cómo utilizar este panel, consulte la Visión general de campos de consulta.
- El panel Condiciones de consulta especifica las condiciones para seleccionar los campos que se listan (por ejemplo, “where VERB = UPDATE”). Para obtener más información sobre cómo utilizar este panel, consulte la Visión general de condiciones de consulta en el tema de ayuda Consultas.

Para obtener información completa, consulte el tema de ayuda de Consultas.

Abrir el Buscador de consultas

Hay un Creador de consultas independiente para cada dominio de informes, por lo que es importante abrir el Creador de consultas correcto. De lo contrario, la información que desee no se visualizará. Todos los dominios se describen en el tema Dominios de los Apéndices de Dominios, Entidades y Atributos.



Después de determinar el dominio a utilizar, pulse Informes > Herramientas de configuración de informes > Creador de consultas.

Búsqueda de una consulta

Existen varias opciones para localizar y ver una definición de consulta en el Creador de consultas:

1. Utilice el Buscador de consultas: consulte el apartado Utilizar el buscador de consultas.
2. Desde un informe que se basa en la consulta, pulse Editar esta consulta del informe en la barra de herramientas del informe.

Utilizar el Buscador de consultas

1. Abra el Buscador de consultas para el dominio adecuado (consulte Abrir el Buscador de consultas).
2. Opcional. Si conoce la Entidad principal para la consulta, selecciónela en la lista.
3. Pulse Buscar.

   Si sólo hay una consulta definida para la Entidad principal seleccionada, dicha consulta se abrirá inmediatamente en el panel de definición de consulta.

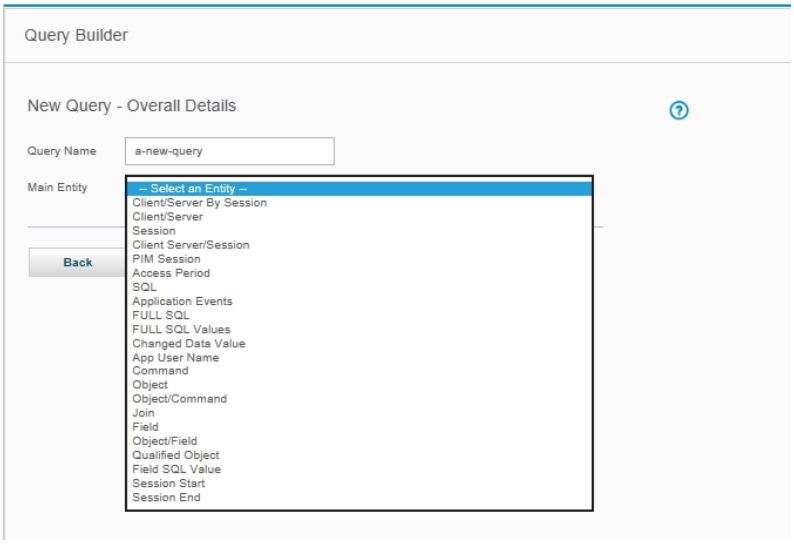
   Si hay varias consultas definidas para la Entidad principal seleccionada, o si no se ha seleccionado ninguna Entidad principal, se visualiza una lista de consultas en el panel Lista de consultas.

   Si se ha seleccionado una Entidad principal para la que no se ha definido ninguna consulta, se le informará.
4. Realice una de las siguientes acciones:

   Para abrir el panel Generador de consultas para una de las consultas listadas, pulse en él. Para definir una consulta nueva, pulse Nueva.

Crear una consulta

1. Abra el Buscador de consultas para el dominio adecuado (consulte Abrir el Buscador de consultas).
2. Pulse Nuevo para abrir el panel Nueva consulta – Detalles generales.
3. Escriba un nombre de consulta exclusivo en el recuadro Nombre de consulta. No incluya caracteres de apóstrofo en el nombre de consulta.
4. Seleccione la entidad principal para la consulta en la lista Entidad principal. La entidad principal controla el nivel de detalle que está disponible para la consulta y que no se puede cambiar. Básicamente, cada fila de datos que devuelve la consulta representa una instancia exclusiva de la entidad principal, y un recuento de apariciones para dicha instancia.
5. Pulse Siguiente. La nueva consulta se abre en el panel Creador de consultas. Para completar la definición, consulte la sección siguiente en Campos de consulta.



Visión general de Campos de consulta

Visión general de Campos de consulta

El panel Campos de consulta lista básicamente las columnas de datos que la consulta devolverá.

Hay dos formas de añadir un campo al panel Campos de consulta:

- Método de menú emergente:

1. Pulse el campo que se va a añadir.
2. Seleccione Añadir campo en el menú emergente.

- Método de arrastrar y soltar:

1. Pulse el icono del campo (no en el nombre del campo).
2. Arrastre el icono a la lista Campos de consulta y suéltelo.

Independientemente del método que se utilice, el campo se añade al final de la lista.

Mover o Eliminar campos en el panel Campos de consulta

Para mover un campo en el panel Campos de consulta:

1. Marque el recuadro de selección para el campo.
2. Utilice los botones siguientes para mover el campo a la ubicación deseada:

   Pulse Arriba para mover el campo una fila hacia arriba.

   Pulse Abajo para mover el campo una fila hacia abajo.

Modificar una consulta

1. Abra el Buscador de consultas para el dominio adecuado (consulte Abrir el Buscador de consultas).
2. Utilice el Buscador de consultas para abrir la consulta que se va a modificar.
3. Consulte el tema Visión general del creador de consultas para modificar cualquier componente de la definición de consulta.

Crear un informe

Una vez que se haya definido una consulta, existen varias opciones para añadir rápidamente un informe tabular que se basa en esa consulta a un diseño de menú existente. Estas opciones sólo se aplican a los informes tabulares.

1. Abra el Buscador de consultas para el dominio adecuado (consulte Abrir el Buscador de consultas).
2. Utilice el Buscador de consultas para abrir la consulta que se va a utilizar para el informe.
3. Realice una de las siguientes acciones:

   Para crear un informe, pulse Crear un informe. Para rehacer un informe tabular existente, pulse Volver a generar.

   Para añadir un informe tabular al separador Mis informes personalizados, pulse Añadir a Mis informes personalizados en el panel. (Si todavía no se ha generado ningún informe tabular para la consulta, primero debe pulsar el botón Crear un informe).

   Para ver datos significativos en el informe tabular, pulse para poder acceder a los parámetros de tiempo de ejecución (cambie la hora a partir de ahora).

Tema principal: Informes

Cómo informar sobre columnas y tablas latentes

Guardium ofrece una funcionalidad que puede ayudar a los arquitectos de datos y DBA a descubrir qué tablas y qué campos no se están utilizando.

Acerca de esta tarea

El concepto básico es el siguiente. Desea saber a qué tablas no se está accediendo. Puede subir todos los nombres de tabla desde la base de datos o desde la Base de datos de gestión de configuración (CMDB) utilizando las funciones de consulta personalizada y el dominio personalizado de Guardium. A continuación, utilice el informe (de la consulta personalizada) para llenar un grupo de objetos.

A continuación, utilice un informe que utilice datos supervisados para mostrar todos los nombres de objeto que han participado en una sentencia SELECT. Hay informes predefinidos para esto en Guardium 8, y todos empiezan por el prefijo DW (Data Warehouse). A continuación, utilice la salida para llenar uno de los grupos predefinidos.

Finalmente, utilice un informe predefinido que muestre todos los miembros del primer grupo que no sean miembros del segundo grupo.

Hay dos conjuntos de dichos informes y grupos: uno que se centra en las tablas y otro que se centra en las tablas y las columnas. La única diferencia es que en los grupos de casos posteriores son de un tipo de 2 tuplas (miembros que son un compuesto de un par de atributos de valor, al que se hace referencia como tupla).

Veamos un ejemplo desde el principio hasta el final que implica una base de datos Oracle y el usuario EMP.

Siga estos pasos.

1. Cargue todos los nombres de tabla y/o todas las combinaciones de tabla/columna del conjunto de tablas de catálogo del sistema (definiciones de los objetos de base de datos).
2. Utilice los datos supervisados para determinar a qué tablas y/o tabla/columnas se ha accedido durante un periodo de tiempo.
3. Cree un informe de todos los elementos del paso 1 que no se encuentran en el paso 2.

Para esta tarea se utilizan las funciones de Guardium siguientes.

- Correlación de datos externos para cargar nombres de tablas y nombres de columnas
- Llenar grupos de consultas
- Creación de informes

Procedimiento

1. Suba todas las tablas desde el catálogo del sistema. Hágalo creando una tabla personalizada.

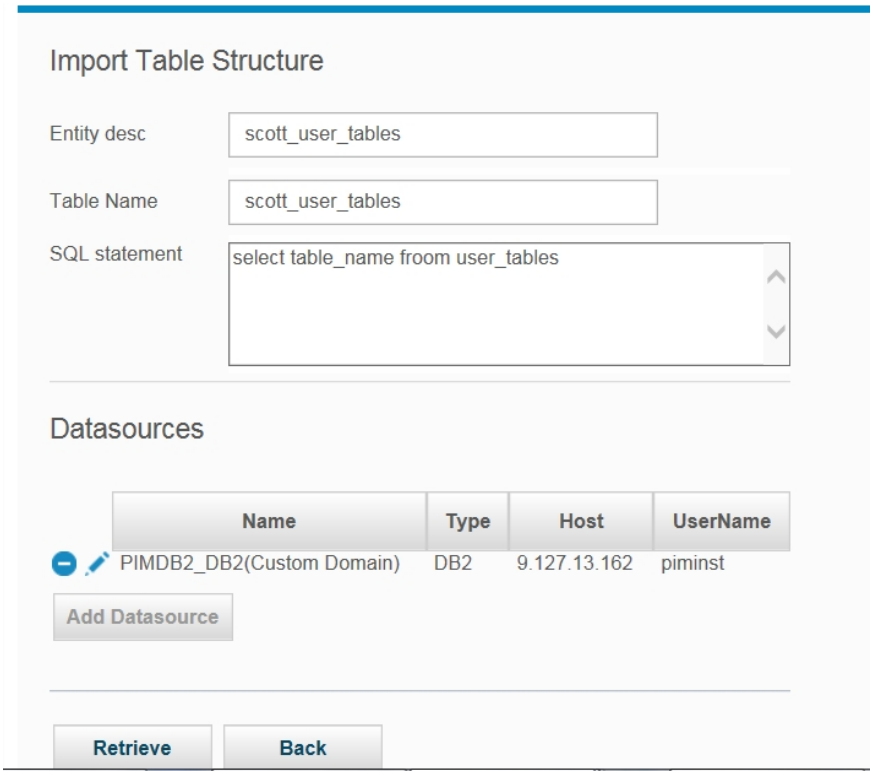
   Requisitos previos

   a. Definir conexión de origen de datos/conexión de base de datos de prueba
   b. Subir datos (crear tabla personalizada)
   c. Crear nuevo dominio (fusionar tablas personalizadas con informes existentes)

   Consulte Correlación de datos externos para obtener más información.

   El ejemplo siguiente está disponible en Cumplir > Informes personalizados > Creador de tablas personalizadas > Definición de carga > Importar estructura de tabla.

   Cuando se haya completado la configuración, pulse el botón Recuperar.



Configuración - Subir definición, Importar estructura de tablas

Cargue los datos para que estén en el sistema Guardium (como una tabla personalizada) y, si lo desea, planifique esta carga. Estos datos se utilizarán para determinar el superconjunto de todas las tablas definidas en el sistema.

Correlacione todos los objetos (y/u objetos-campos) del sistema

En este ejemplo, se utilizan datos latentes basados en nombres de tabla. Pero el análisis puede incluir columnas, siempre que las tareas de carga estén definidas para devolver los pares de `<object,field>` y utilicen grupos de tuplas para compararlos con una tupla observada de `object+field`.

Para las instancias de Objeto-Campo, sustituya el informe Objetos latentes de DW por el informe Objetos-campos latentes de DW. Para las instancias de Objeto-campo, sustituya el informe Acceso a objetos de DW SELECT por el informe Acceso de objeto-campo de DW.

Una vez que haya completado la carga, defina un dominio personalizado basado en esta tabla personalizada única y defina un informe que recupere los nombres de tabla.

A continuación, rellene el grupo Todos los objetos de DW a partir de este informe y planifique esta acción Importar desde consulta si lo desea. Esto crea un grupo que tiene todas las tablas según lo definido por el catálogo del sistema.

Nota: Al llenar el grupo Todos los objetos de DW de grupo, debe incluir la información para pulsar Ejecutar una vez ahora -> Seleccionar todo -> Pulse el botón Importar. Haga lo mismo para el nombre de grupo "Objetos accedidos de DW SELECT". Tiene que importar todas las definiciones planificadas.

Cuando haya terminado, pulse el botón Guardar.

2. Correlación directa del objeto

   Utilice los datos supervisados para determinar a qué tablas y/o tabla/columnas se ha accedido durante un periodo de tiempo.

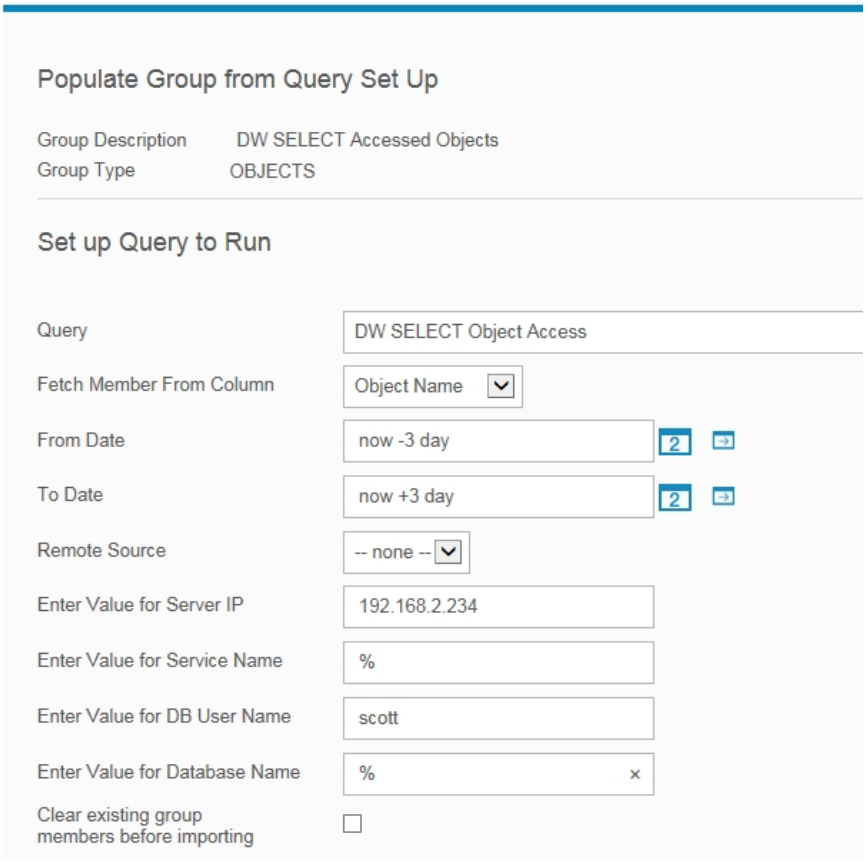
   Consulte algunos informes predefinidos adicionales. El informe Acceso a objetos de DW SELECT muestra todos los nombres de objetos a los que se ha accedido mediante una sentencia SELECT.

   Ahora, rellene el grupo Objetos accedidos de DW SELECT del informe, rellenando los atributos de filtrado que necesite.

   Nota: Al llenar el grupo Todos los objetos de DW, debe incluir la información para pulsar 'Ejecutar una vez ahora' -> Seleccionar todo -> Pulse el botón Importar. Haga lo mismo para el nombre de grupo "Objetos accedidos de DW SELECT". Tiene que importar todas las definiciones planificadas.

   El ejemplo siguiente está disponible en Configuración > Herramientas y vistas > Creador de grupos > Elegir Todos los objetos de DW > Cumplimentar desde consulta > Acceso a objetos de DW SELECT.

   Cuando haya terminado, pulse el botón Guardar.



Configuración - Cumplimentar grupo desde consulta, Nombre de objeto

3. Cree un informe de todos los elementos del paso 1 que no se encuentran en el paso 2.

   Utilice el informe Objetos latentes de DW para ver objetos que se encuentran en el grupo todos los objetos, pero que no se han utilizado en una Selección.

   Compare este informe con el informe anterior - Nombres de tabla. Observe que EMP no está en este informe porque se ha utilizado en una sentencia SELECT.

   Nota: Puesto que los miembros del grupo se gestionan y se sincronizan centralmente entre el Gestor central y las unidades gestionadas, el contenido de este informe se puede retrasar hasta 30 minutos. Si necesita acceder a la información que está más actualizada, ejecute este informe en el Gestor central o solicite al administrador de Guardium que sincronice la unidad gestionada desde el Gestor central.

   Más formas de acceder a las tablas

   Correlación de objetos indirectamente

   Además de acceso directo a SELECT, es posible que se pueda acceder a las tablas a través de funciones y procedimientos almacenados. En este caso, tendrá que hacer un poco más de correlación para permitir que Guardium calcule estos tipos de SELECT.

   En primer lugar, utilice el informe Acceso a objetos de DW EXECUTE para rellenar el grupo denominado Objetos de DW EXECUTE con un conjunto de nombres de procedimientos almacenados que se están ejecutando. A continuación, utilice la correlación indirecta para generar todos los objetos que se utilizan desde estos procedimientos.

   Suponga que tiene un procedimiento definido:

```
create or replace procedure num_depts(deptnums out NUMBER) is
begin
    select count(*) into deptnums from dept;
end;
```

   En este caso, cada ejecución de num_depts también realiza una selección en DEPT.

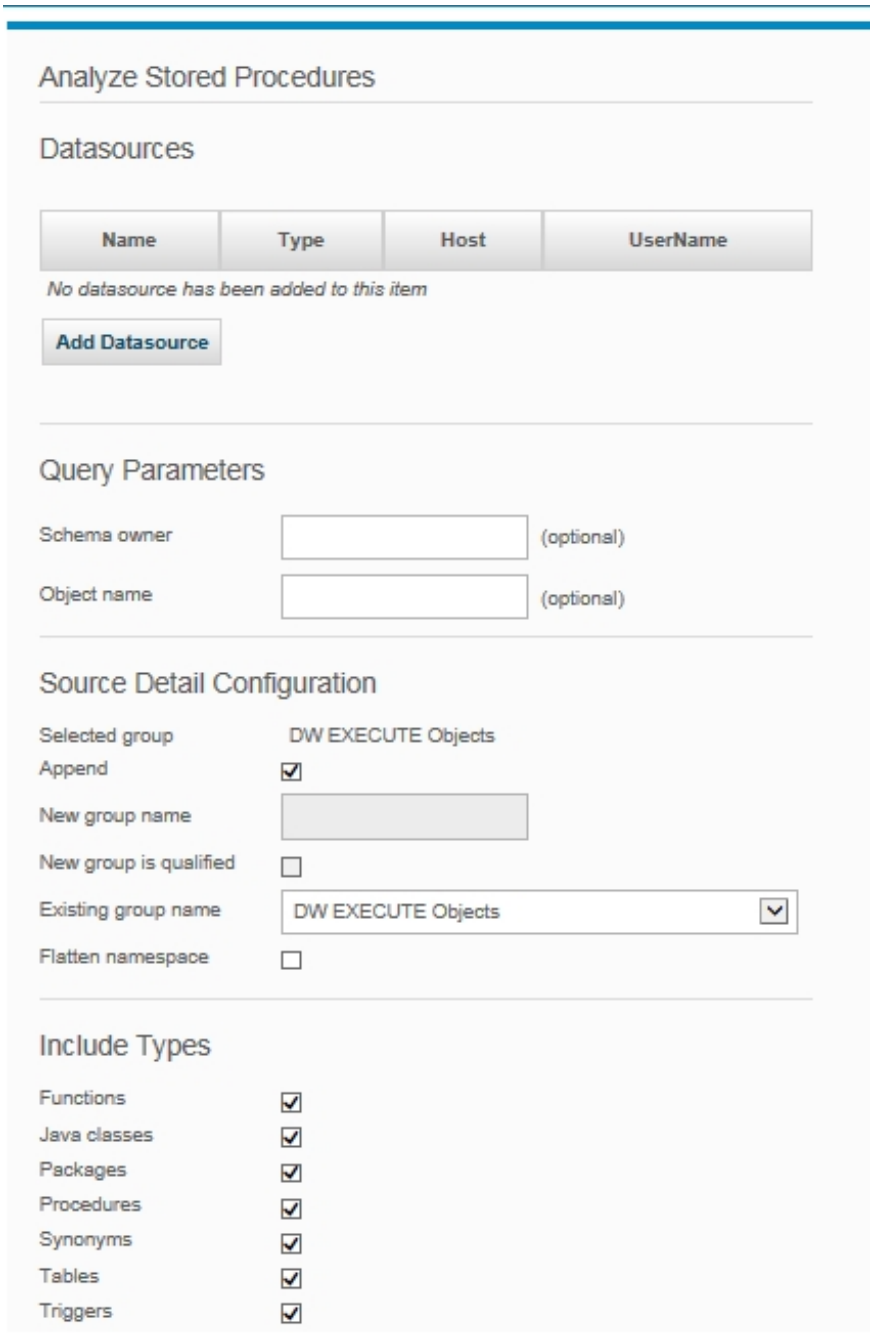
   Utilice la característica “cumplimentar grupo desde consulta” para utilizar la columna Nombre de objeto en el informe Acceso a objetos de DW EXECUTE para llenar el grupo “Objetos ejecutados de DW”. A continuación, utilice este grupo para llenar el grupo de Objetos accedidos de DW EXECUTE.

   En el Creador de grupos, seleccione los Objetos DW EXECUTE de la lista y pulse en Proxy de llamada generado automáticamente. Seleccione Utilizar dependencias inversas, que sólo está soportado para Oracle en Guardium 8, o bien Generar objetos seleccionados.

   Si opta por utilizar dependencias, tendrá que elegir una base de datos que tenga acceso a DBA_DEPENDENCIES y el tipo de dependencias que deben seguirse.

   Elija añadir miembros al grupo Objetos accedidos de DW EXECUTE.

   El ejemplo siguiente está disponible en Configuración > Herramientas y vistas > Creador de grupos > Elegir Objetos accedidos de DW EXECUTE > Proxy de llamada generado automáticamente > Utilizando dependencias inversas > Analizar procedimientos almacenados.



Configuración - Proxy de llamada generado automáticamente, Utilizando dependencias inversas

Esto añadirá los objetos dependientes al grupo Objetos accedidos de DW EXECUTE.

Tema principal: Informes

Cómo generar la Llamada de API desde Informes

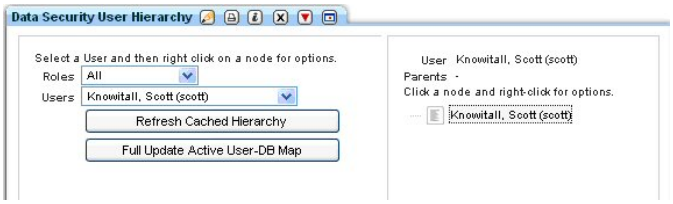
Generar llamadas de API de Guard desde un informe, ya sea desde una sola fila dentro de un informe o basándose en el informe

Valor añadido: A través de una interfaz gráfica de usuario, utilizando los datos existentes en el sistema que se visualiza en los informes como parámetros para las llamadas de API, generar y llenar llamadas de API de forma rápida y sencilla sin tener que ejecutar mandatos de nivel de sistema ni escribir llamadas de API largas para realizar operaciones como crear orígenes de datos, definir motores de inspección, mantener jerarquías de usuario o mantener las funciones de Guardium, como por ejemplo S-TAP.

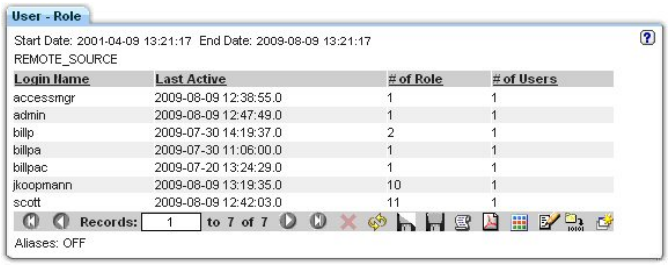
Llamada a la API de una sola fila

Para este escenario, generaremos llamadas de función de API para llenar la Jerarquía de usuario de seguridad de datos.

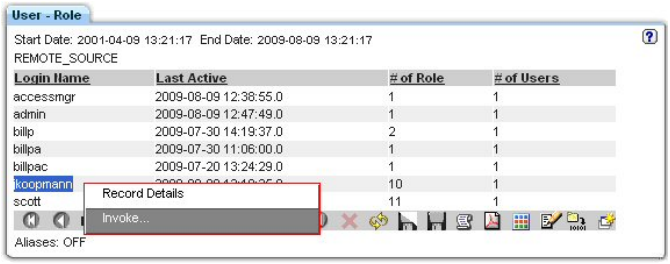
1. Para empezar, mostremos la **Jerarquía de usuarios de seguridad de datos** actual para el usuario **scott**



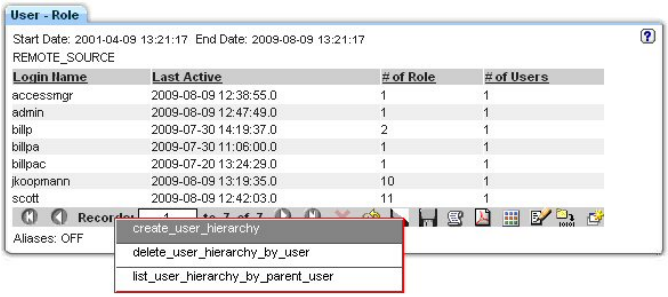
2. Para invocar una función de API debemos encontrar un informe que tenga actualmente las funciones de API deseadas enlazadas. Puesto que la creación de una jerarquía de usuario está relacionada con los usuarios, la selección de un informe de usuario debe producir resultados correctos. Para este escenario, hemos seleccionado el informe **Usuario - Rol**.



3. **Al efectuar una doble pulsación sobre una fila** para detallar más, se mostrará una opción para **Invocar...**

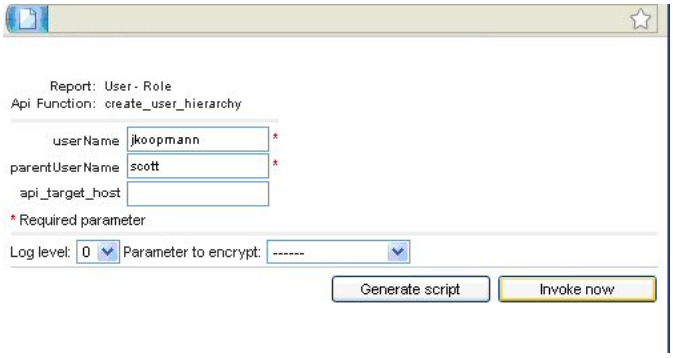


4. Pulse en la opción **Invocar...** para visualizar una lista de funciones de API que están correlacionadas con este informe



5. Pulse en la **API** que le gustaría invocar; abriendo el Formulario de llamada de API para el Informe y la Función de API invocada

6. Rellene los parámetros necesarios y los parámetros no necesarios para la llamada de API seleccionada. Muchos de los parámetros se rellenan previamente desde el informe, pero se pueden cambiar para crear una llamada de API exclusiva. Para obtener ayuda específica para rellenar los parámetros necesarios o no necesarios, consulte las llamadas de función de API individuales dentro de la guía de Referencia de GuardAPI.



7. Utilice la lista desplegable para seleccionar el **Nivel de registro**, donde el Nivel de registro representa lo siguiente (0 - devuelve ID=*identificador* y ERR=*error_code* tal como se define en los Códigos de retorno, 1 - muestra información adicional en pantalla, 2 - pone información en los registros de depuración de la aplicación Guardium, 3 - hará ambos)

8. Utilice la lista desplegable para seleccionar un **Parámetro que se va a cifrar**.

Nota: El cifrado de parámetros se habilita estableciendo el Secreto compartido y sólo es relevante para invocar la función de API a través de la generación de scripts.

9. Elija **Invocar ahora** o **Generar script.**

   a. Si se selecciona **Invocar ahora**, la llamada a la API se ejecutará inmediatamente y mostrará una pantalla de Salida de llamada de API que muestra el estado de la llamada de API.

   b. Si **Generar script** está seleccionado: Abra el script generado con su editor favorito u, opcionalmente, guárdelo en disco para editarlo y ejecutarlo más adelante -- sustituyendo cualquiera de los valores de parámetro vacíos (indicados por '< >') si están contenidos en el script.
   Nota: Los parámetros vacíos pueden permanecer en el script ya que la llamada a la API los ignorará

   Script de ejemplo

   # Un script de plantilla para invocar la función guardAPI create_user_hierarchy :

   # Uso: ssh cli@a1.corp.com<create_user_hierarchy_api_call.txt

   # sustituya cualquier < > por el valor obligatorio

   #

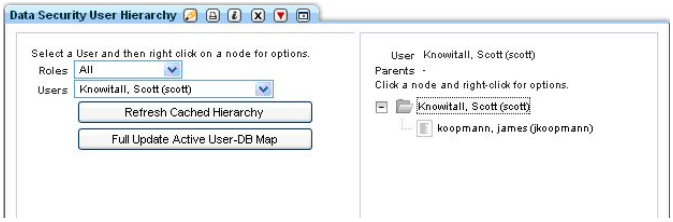
   grdapi create_user_hierarchy userName=jkoopmann parentUserName=scott

   c. Ejecute la llamada de función de CLI.

   Llamada de ejemplo

   $ ssh cli@a1.corp.com<create_user_hierarchy_api_call.txt

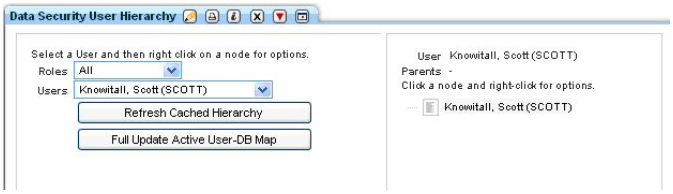
10. Validar. En este escenario, es una nueva visualización de la Jerarquía de usuarios de seguridad de datos.



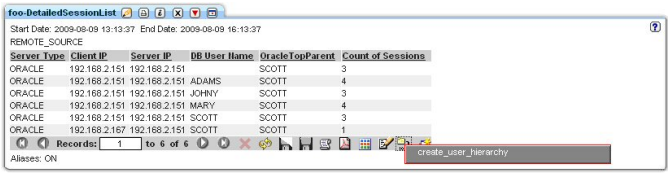
Llamada a la API de varias filas

Este caso de ejemplo utiliza un informe personalizado con parámetros correlacionados para campos de informe. Consulte los escenarios adicionales de esta sección para obtener información adicional.

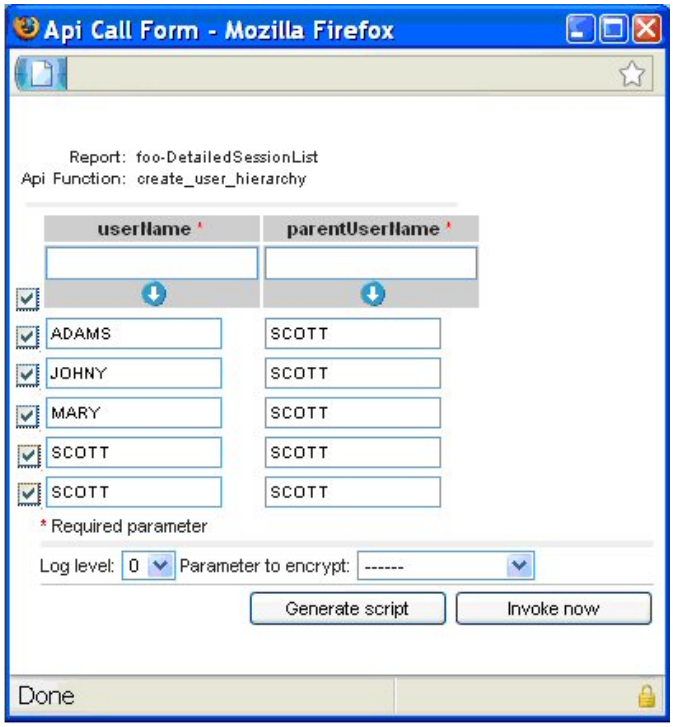
1. Para empezar, vamos a mostrar la **Jerarquía de usuarios de seguridad de datos** actual para el usuario **scott**



2. Pulse en el icono **Invocar...** para visualizar una lista de las API que están correlacionadas con este informe



3. Pulse en la **API** que le gustaría invocar; abriendo el formulario de llamadas de API para el informe y la función de API invocada. Invocar una llamada de API desde un informe para varias filas generará un formulario de llamadas de API que visualice y habilite la edición de todos los registros visualizados en la pantalla (en función del tamaño de captación) hasta un máximo de 20 registros.



4. Utilice los **recuadros de selección** para seleccionar/deseleccionar las filas que van a ser destino de la llamada de API.

5. Rellene los **parámetros necesarios** y los **parámetros no necesarios** para la llamada de API seleccionada. Muchos de los parámetros se rellenan previamente desde el informe, pero se pueden cambiar para crear una llamada de API exclusiva. Para obtener ayuda específica para rellenar los parámetros necesarios o no necesarios, consulte las llamadas de función de API individuales dentro de la guía de Referencia de GuardAPI. Además, utilice el conjunto de parámetros de la API para especificar un valor para un parámetro y, al pulsar en el botón de flecha hacia abajo, para rellenar ese parámetro para todos los registros.

6. Utilice la lista desplegable para seleccionar el **Nivel de registro**, donde el Nivel de registro representa lo siguiente (0 - devuelve ID=*identificador* y ERR=*error_code* tal como se define en los Códigos de retorno, 1 - muestra información adicional en pantalla, 2 - pone información en los registros de depuración de la aplicación Guardium, 3 - hará ambos)

7. Utilice la lista desplegable para seleccionar un **Parámetro que se va a cifrar**.
Nota: El cifrado de parámetros se habilita estableciendo el Secreto compartido y sólo es relevante para invocar la función de API a través de la generación de scripts.

8. Elija **Invocar ahora** o **Generar script.**

    a. Si se selecciona **Invocar ahora**, la llamada a la API se ejecutará inmediatamente y mostrará una pantalla de Salida de llamada de API que muestra el estado de la llamada de API. En este escenario, las dos últimas llamadas de API fallarán porque no pueden tener una relación cíclica en la jerarquía.

    b. Si **Generar script** está seleccionado: Abra el script generado con su editor favorito u, opcionalmente, guárdelo en disco para editarlo y ejecutarlo más adelante -- sustituyendo cualquiera de los valores de parámetro vacíos (indicados por '< >') si están contenidos en el script. Con este escenario, podríamos suprimir fácilmente las dos últimas líneas del script -- sabiendo que crearían errores cíclicos.
    Nota: Es posible que los parámetros vacíos permanezcan en el script ya que la llamada a la API los ignorará.

    Script de ejemplo

    # Un script de plantilla para invocar la función guardAPI create_user_hierarchy :

    # Uso: ssh cli@a1.corp.com<create_user_hierarchy_api_call.txt

    # sustituya cualquier < > por el valor obligatorio

    #

    grdapi create_user_hierarchy userName=ADAMS parentUserName=SCOTT

    grdapi create_user_hierarchy userName=JOHNY parentUserName=SCOTT

    grdapi create_user_hierarchy userName=MARY parentUserName=SCOTT

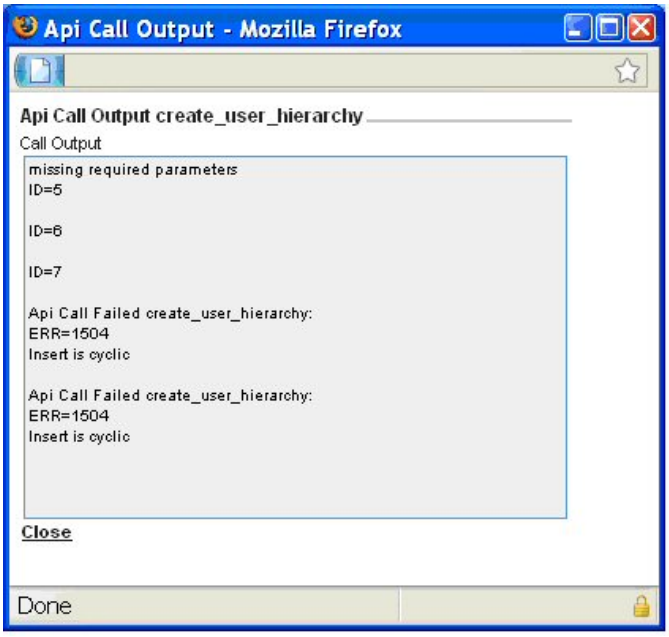
    grdapi create_user_hierarchy userName=SCOTT parentUserName=SCOTT

    grdapi create_user_hierarchy userName=SCOTT parentUserName=SCOTT

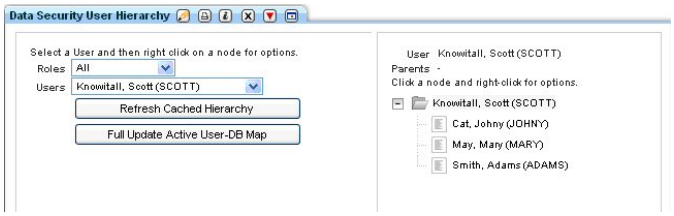
    c. Ejecute la llamada de función de CLI.

    Llamada de ejemplo

    $ ssh cli@a1.corp.com<create_user_hierarchy_api_call.txt



9. Validar. En este escenario, es una nueva visualización de la Jerarquía de usuarios de seguridad de datos.



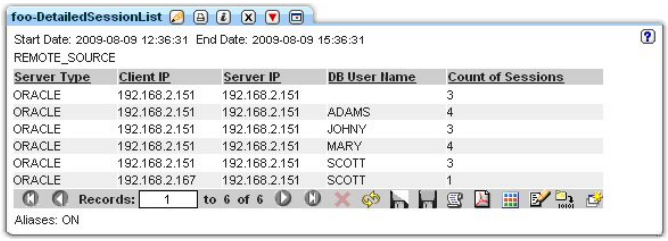
Tema principal: Informes

Cómo utilizar Constantes en Llamadas de API

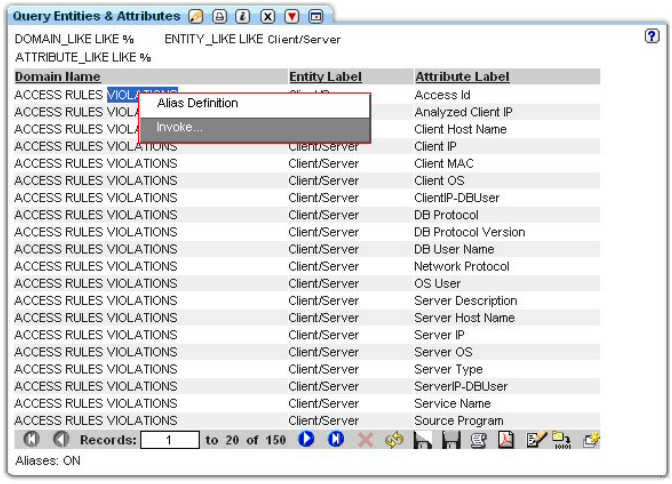
Cree un atributo de entidad nuevo que se utilizará durante una llamada de función de API.

Valor añadido: A través de una interfaz gráfica de usuario, cree una constante definida por el usuario que se pueda utilizar para rellenar un parámetro en una llamada a función de API.

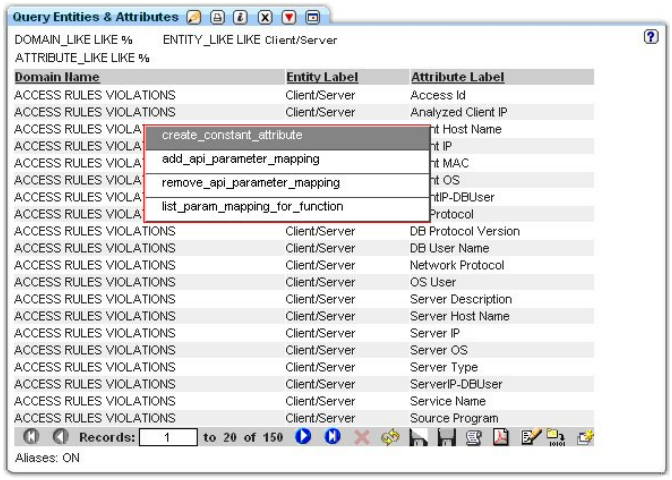
1. Desde nuestro informe, podemos modificarla para que tenga un campo que podamos utilizar para las correlaciones de parámetros.



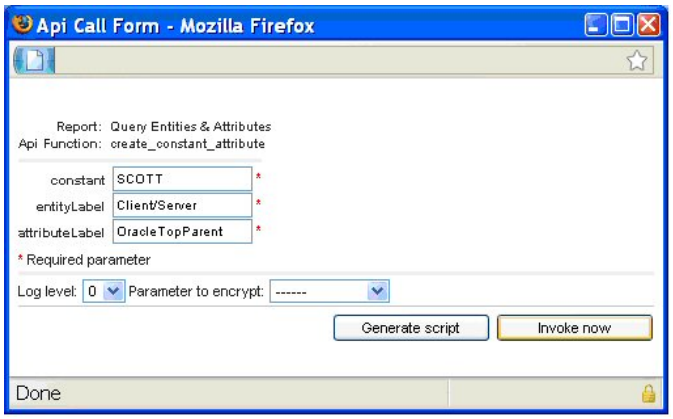
2. Vaya al informe Entidades y atributos de consulta para la entidad Cliente/Servidor dentro del dominio INFRACCIONES DE REGLAS DE ACCESO. Efectúe una doble pulsación sobre una fila y seleccione la opción Invocar...



3. Invoque la función de la API create_constant_attribute.

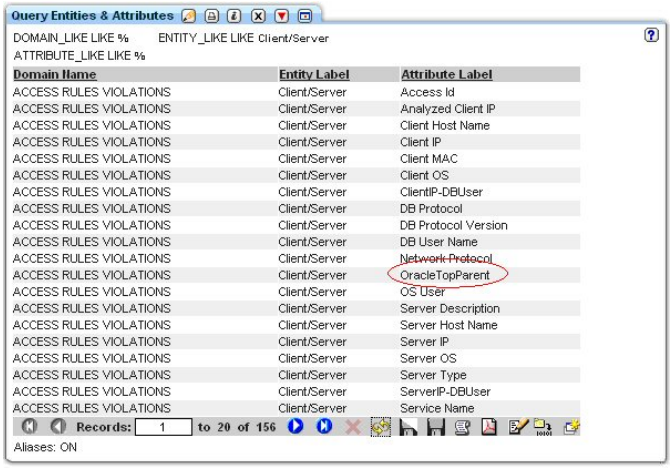


4. Rellene el valor de la constante que se va a utilizar ('SCOTT'), rellene attributeLabel a lo que desee llamarlo ('OracleTopParent') y, a continuación, pulse el botón Invocar ahora para crear la constante.

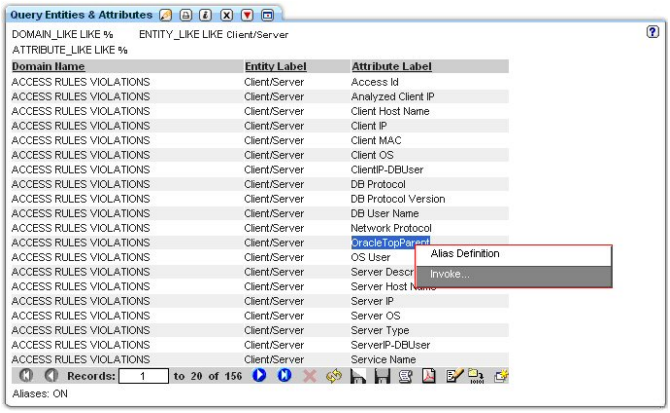


5. Al pulsar en el botón Invocar ahora se producirá un estado Salida de llamada de API que muestra la constante creada.

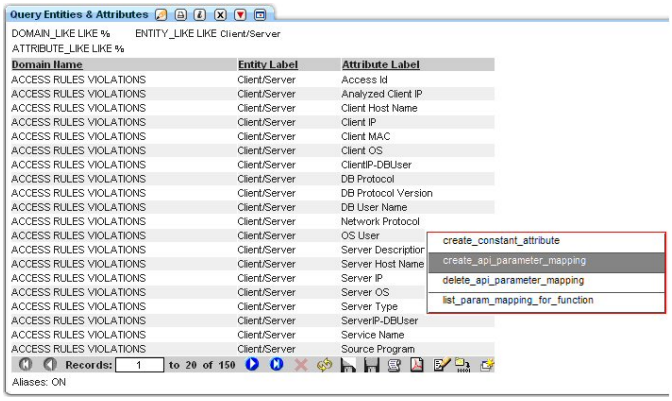
6. Una nueva visualización del informe Entidades y atributos de consulta mostrará el nuevo atributo creado.



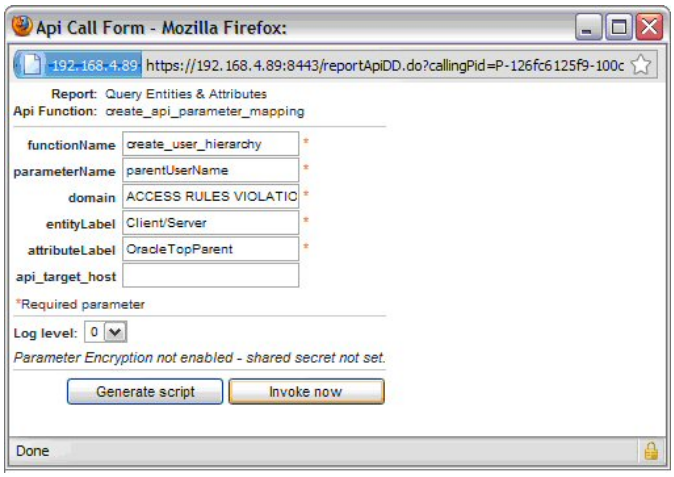
7. La constante que se acaba de crear ahora se puede correlacionar para el informe. Efectúe una doble pulsación en la nueva fila y seleccione la opción Invocar...



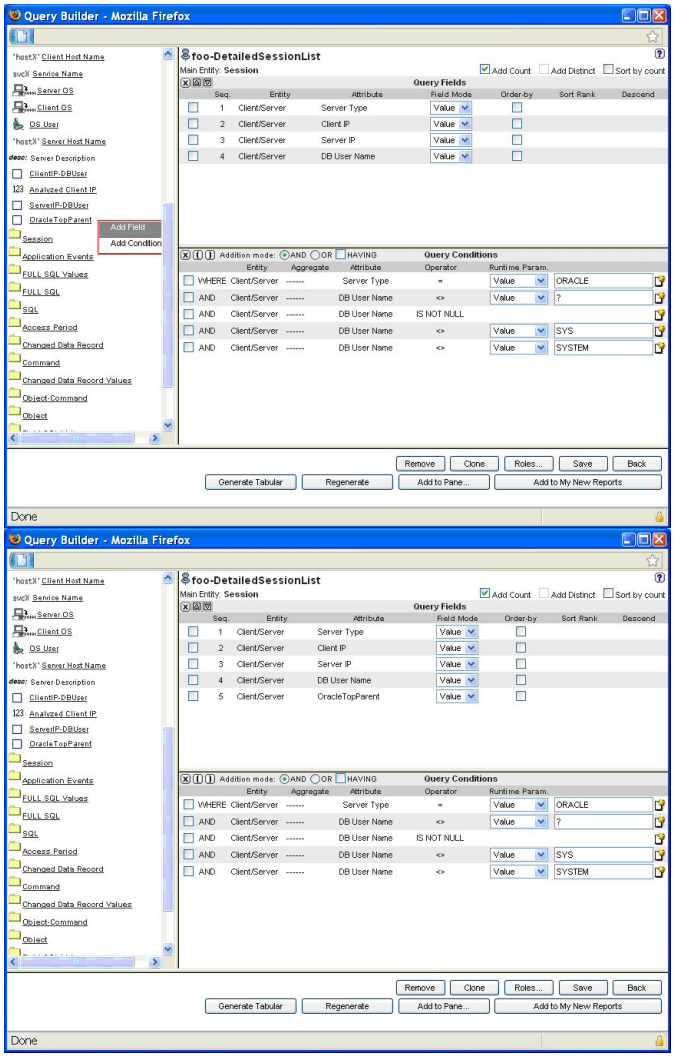
8. Seleccione la opción create_api_parameter_mapping.



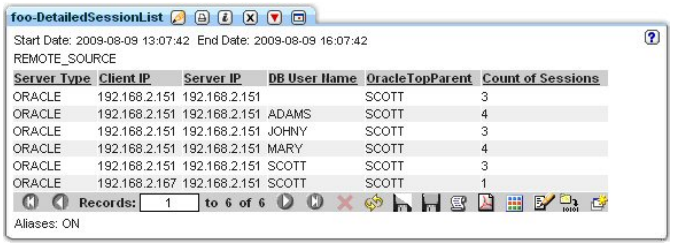
9. Rellene functionName y parameterName y pulse el botón Invocar ahora.



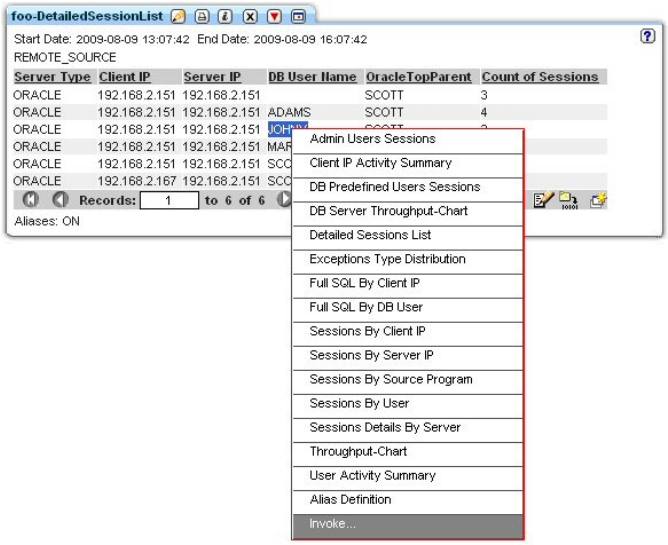
10. El atributo recién creado se debe añadir al informe. Edite la consulta a través del Creador de consultas y añada el campo.



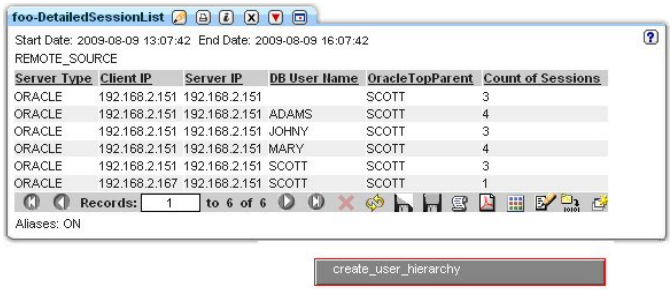
11. Ahora, cuando se visualice el informe, se visualizará el nuevo atributo.



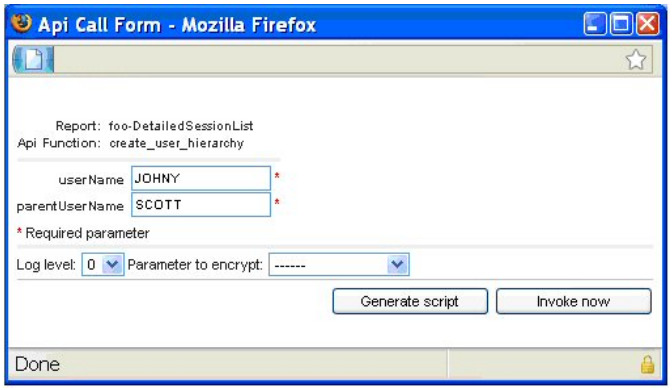
12. Para validar el uso de la constante nueva, efectúe una doble pulsación en una fila y seleccione la opción Invocar...



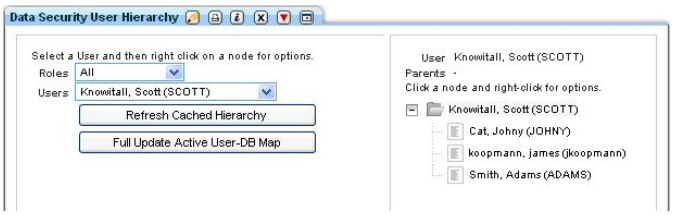
13. Seleccione la función de API



14. Ahora, el parentUserName se rellena a partir de la constante recién añadida. Pulse el botón Invocar ahora.



15. Valide la nueva Jerarquía de usuarios de seguridad de datos.



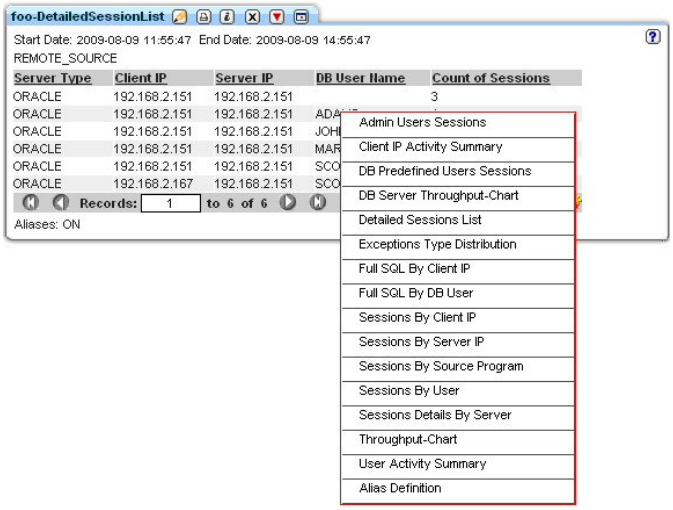
Tema principal: Informes

Cómo utilizar llamadas de API desde informes personalizados

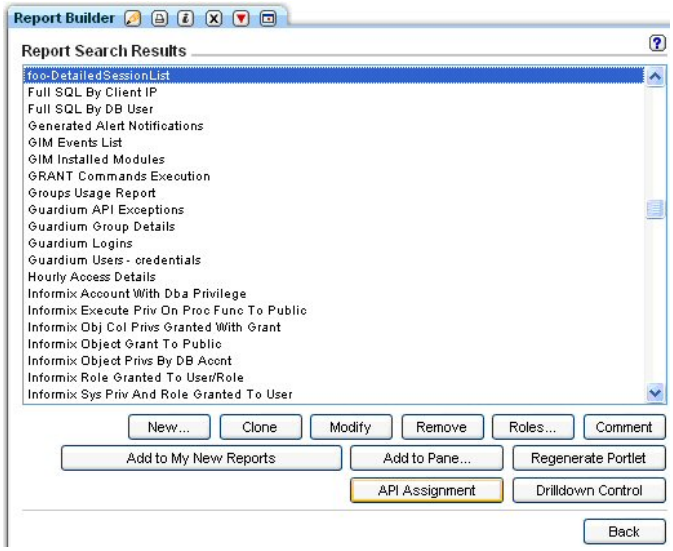
Enlace funciones de API con informes y correlacione campos de informe con los parámetros funcionales de la API.

Valor añadido: A través de una interfaz gráfica de usuario, correlacione rápida y fácilmente parámetros de la API con campos de informe personalizados que se utilizarán en las llamadas a función de la API.

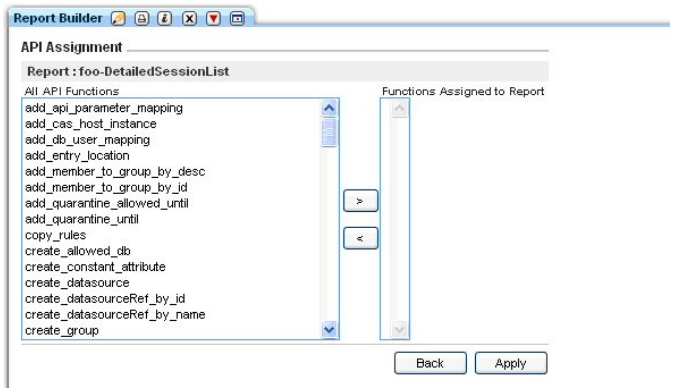
1. De forma predeterminada, un informe personalizado que se acaba de crear no tendrá ninguna función de API enlazada a él. Esto puede ser visto por el informe personalizado siguiente, en el que una doble pulsación en una fila sólo generará una lista de informes de detalles adicionales para ejecutar pero le falta la opción Invocar.



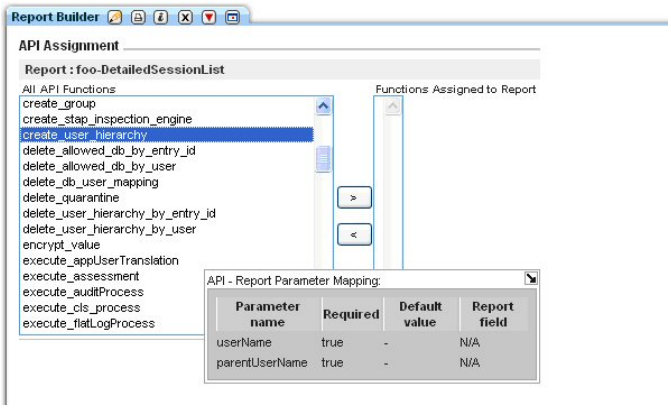
2. El enlace de las funciones de API con los informes se realiza a través del Creador de informes de Guardium. Abra el Creador de informes, busque su informe personalizado y, a continuación, pulse el botón Asignación de API.



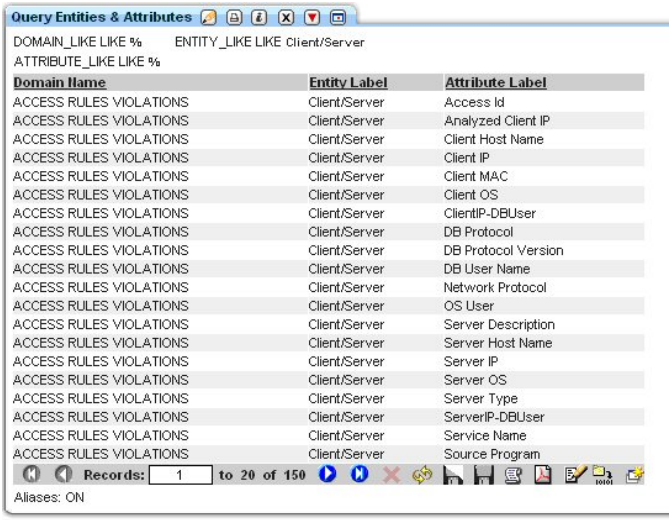
3. El panel Asignación de API muestra todas las funciones de API asignadas al informe seleccionado. Observe que para nuestro escenario el informe seleccionado no tiene funciones de API asignadas.



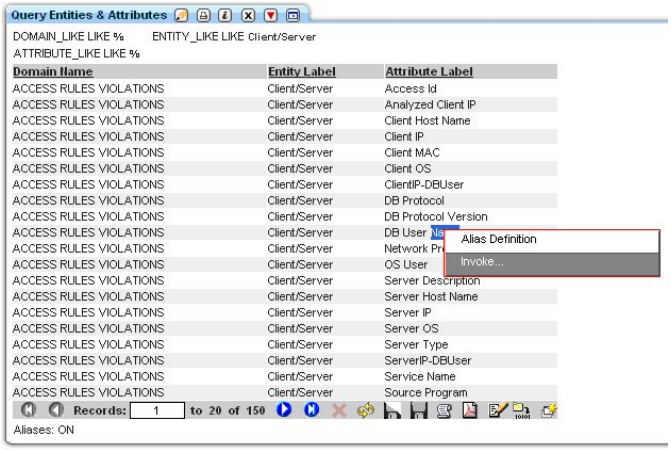
4. Para asignar una función de API a un informe, busque una API que desee enlazar con el informe, pulse la flecha mayor que y, a continuación, pulse el botón Aplicar. Para nuestro escenario, hemos seleccionado create_user_hierarchy. Cuando se seleccione, aparecerá una ventana emergente que muestra las correlaciones de parámetros de informe (cuyos campos de informes se utilizarán al llamar a la función de la API). Observe que no hay campos de informes correlacionados en nombres de parámetros.



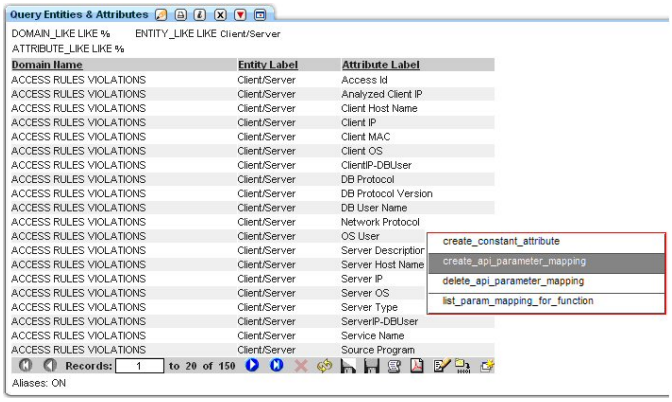
5. En este punto, ninguno de los campos de informe está correlacionado con los parámetros de la API. Los usuarios pueden ir al informe Entidades y atributos de consulta para crear estas correlaciones; de lo contrario, cuando se invoque la llamada de API, ninguno de los parámetros tendrá valores. Añada las correlaciones de parámetros de la API. Abra el informe Entidades y atributos de consulta y cree las correlaciones. Puesto que nuestro informe para este escenario utiliza la entidad Cliente/Servidor dentro del dominio INFRACCIONES DE REGLAS DE ACCESO, filtre el informe utilizando el botón Personalizar; modificando el informe para que sólo se muestre la entidad Cliente/Servidor.



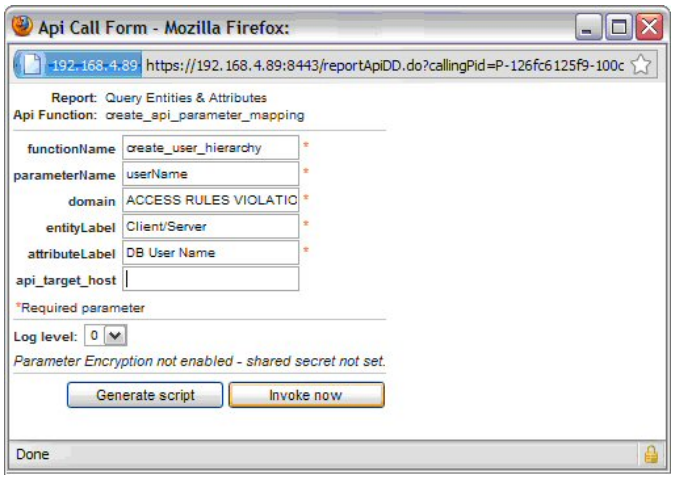
6. Efectúe una doble pulsación en el atributo que desee asignar a un nombre de parámetro y pulse la opción Invocar...



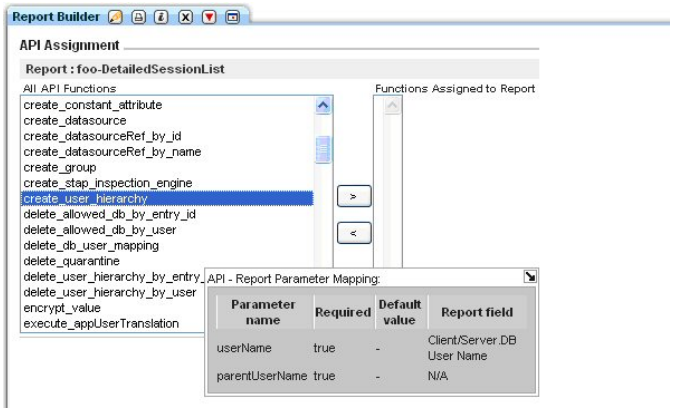
7. Seleccione la función de API create_api_parameter_mapping.



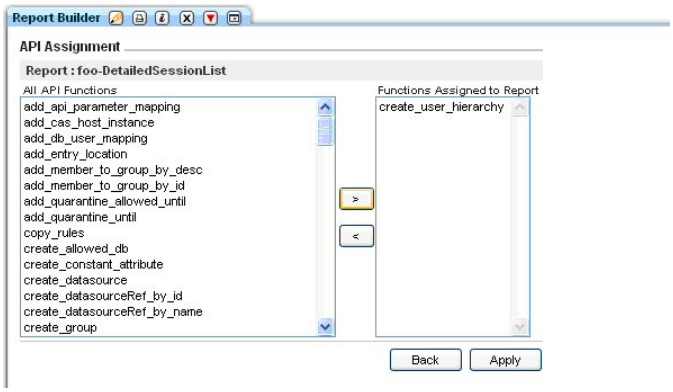
8. Rellene functionName y parameterName en el Formulario de llamada de API y pulse el botón Invocar ahora.



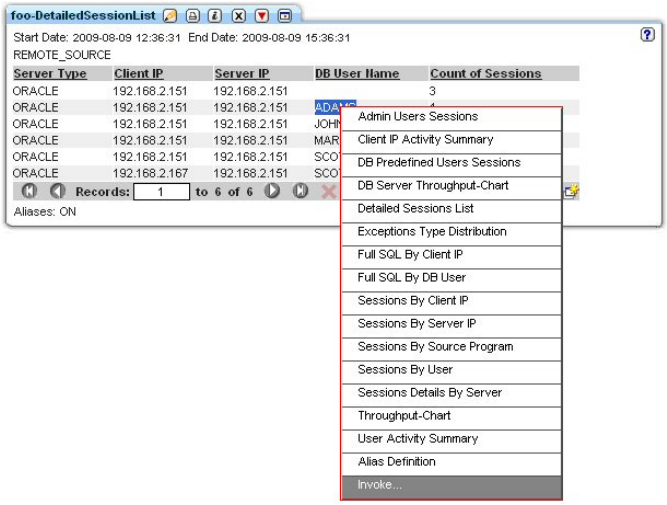
9. Ahora, cuando vuelva al Creador de informes para nuestro informe y observe la Asignación de API; al pulsar en la función de API create_user_hierarchy se muestra la API - Correlación de parámetros de informe con nuestra correlación de userName con el campo Informe del Nombre de usuario de BD de Cliente/Servidor.



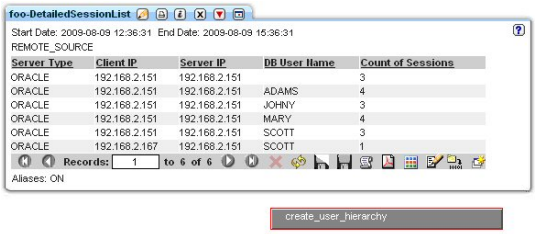
10. Pulse en la flecha mayor que '>' y pulse el botón Aplicar



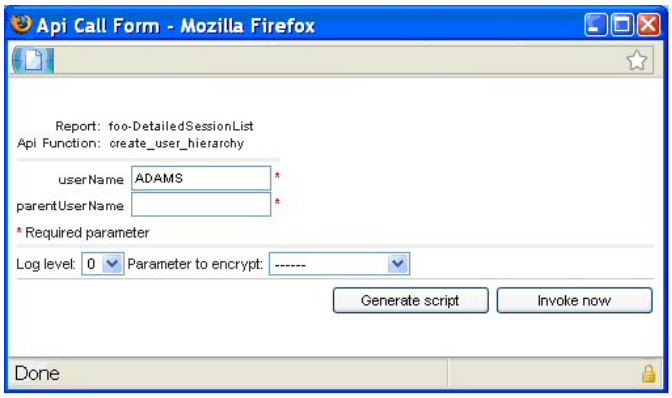
11. Ahora, cuando invocamos la función de API create_user_hierarchy a través de nuestro informe, el parámetro userName se rellenará a partir del informe. Para verlo, vuelva al informe y efectúe una doble pulsación en una fila y, a continuación, pulse la opción Invocar...



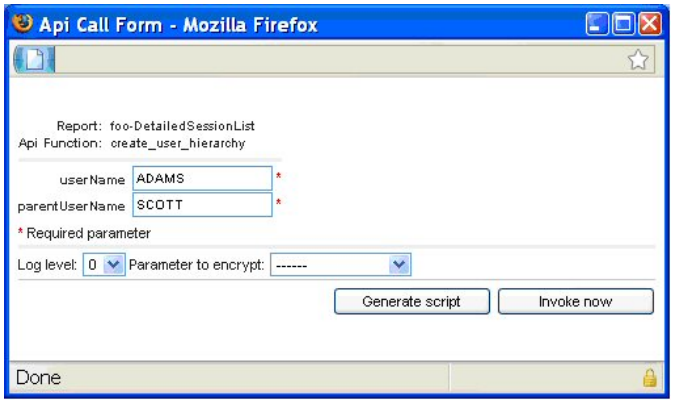
12. Pulse en la función de la API (en nuestro caso, create_user_hierarchy).



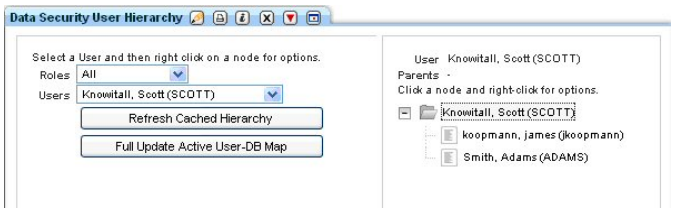
13. Observe que el userName se ha rellenado ahora a partir del campo de informe.



14. Rellene el parentUserName y pulse el botón Invocar ahora.



15. Verifique que se haya añadido la nueva Jerarquía de usuarios de seguridad de datos.



Tema principal: Informes

Canal de información externo opcional

Los canales de información externos le permiten enviar los datos del informe de Guardium directamente a una base de datos externa.

El envío de datos de informes a una base de datos externa es útil en varios escenarios, por ejemplo, al combinar o correlacionar datos de Guardium con datos que no son de Guardium, cuando se utilizan datos de Guardium con herramientas externas de creación de informes o cuando se registran registros de análisis de máquina en informes de gran tamaño.

Antes de utilizar canales de información externos, verifique los requisitos previos siguientes:

- Correlacione un canal de información entre Guardium y una base de datos externa. Los canales de información externos soportan actualmente bases de datos relacionales y es posible que no funcionen con otros tipos de base de datos.
- Cree un informe que defina los datos que se deben enviar a través del canal de información externo. Los informes predefinidos no funcionarán con canales de información externos. Si desea utilizar informes predefinidos, realice una copia con el informe y utilice la copia para el canal de información externo.
- Defina un proceso de auditoría que utilizará el canal de información externo.

La primera vez que se ejecuta una tarea opcional de canal de información externo, se creará la representación interna necesaria de los orígenes de auditoría. Una limitación es que los datos que tienen una indicación de fecha y hora con una fecha anterior a la fecha de creación del origen de auditoría no se pueden almacenar. Esto significa que la primera vez que se ejecuta la tarea, ésta sólo exportará datos para la fecha actual. En ejecuciones posteriores de la tarea después de esa fecha, se puede exportar cualquier dato a partir de esa fecha. (En otras palabras, al día siguiente podrá exportar los datos de ese día más los datos del día anterior).

Crear una tarea de canal de información externo opcional

Si aún no ha empezado a definir un proceso de automatización del flujo de trabajo de cumplimiento, consulte el apartado Crear un proceso de flujo de trabajo antes de realizar este procedimiento.

1. Si el panel Añadir tarea nueva no está abierto, pulse Añadir tarea de auditoría.
2. Pulse Canal de información externo.
3. Seleccione el tipo de canal de información en la lista Tipo de canal de información. (Los controles que aparecen a continuación dependen del tipo de canal de información seleccionado). Un tipo de canal de información predefinido es Último objeto referenciado.
   Nota: Debe correlacionar un canal de información externo antes de intentar utilizar esta característica.
4. Seleccione un tipo de suceso en la lista Tipo de suceso.
5. Seleccione un informe desde la Lista de informes. En función del informe seleccionado, se muestra un número variable de parámetros en el panel Parámetros de tarea.
6. En el recuadro Retardo de extracción, especifique el número de horas por las que se va a retrasar el canal de información y marque el recuadro Continuo para incluir los datos hasta el momento en que se ejecuta la tarea de auditoría. La opción Retardo de extracción sólo funciona cuando se marca el recuadro Continuo.
7. En el panel Orígenes de datos, identifique uno o más orígenes de datos para el canal de información externo. Para obtener instrucciones acerca de cómo definir o seleccionar orígenes de datos, consulte Orígenes de datos.
8. Especifique todos los valores de parámetro en el panel Parámetros de tarea. Los parámetros variarán en función del informe seleccionado. La columna de recuento no está soportada en el Canal de información externo.
9. Pulse Aplicar.

Tema principal: Informes
Conceptos relacionados:
Creación de procesos de auditoría
Tareas relacionadas:
Correlación de un canal de información externo

Correlación de un canal de información externo

Aprenda a correlacionar un canal de información externo para enviar datos de informes de Guardium directamente a una base de datos externa.

Antes de empezar

Verifique los requisitos previos siguientes antes de correlacionar un canal de información externo:

- Identifique la base de datos externa que recibirá los datos del canal de información y recopile la información de conexión necesaria para dicha base de datos (dirección IP, número de puerto, nombre de usuario, contraseña, etc.). Los canales de información externos soportan actualmente bases de datos relacionales y es posible que no funcionen con otros tipos de base de datos.
- Identifique el informe de Guardium que proporcionará datos al canal de información externo.
-

Acerca de esta tarea

Los canales de información externos le permiten enviar información de informes de Guardium directamente a una base de datos externa. Todo lo que se pueda definir en un informe se puede enviar a través de un canal de información externo. Estos canales de información dependen de la correlación DOMAIN_ID y ATTRIBUTE_ID del mecanismo de creación de informes de Guardium con los campos de tabla de la base de datos externa. Cada correlación consta de los registros de cuatro tablas

(EF_MAP_TYPE_HDR, EF_MAP_TABLE, EF_MAP_COLUMN y EF_MAP_GDM_TYPE). Utilice la función grdapi_create_ef_mapping para ayudar a crear estas tablas y establecer la correlación.

Procedimiento

1. Genere un informe con los datos que le gustaría transferir utilizando un canal de información externo. Puede hacer esto desde un gestor central, un agregador o una instancia autónoma de Guardium, siempre que el sistema pueda acceder a los datos de informe que necesite.
2. Desde la CLI, ejecute `grdapi create_ef_mapping reportName="My report"`. Además de establecer la correlación, la función grdapi_create_ef_mapping también genera una sentencia create table de ejemplo que se utilizará en los pasos posteriores.
3. En el sistema Guardium en el que se ha definido el informe, busque en /var/log/guard un nombre de archivo como ef_sample_[my_report].sql. Este archivo contiene las sentencias create table de ejemplo. Debe modificar las sentencias de este archivo para que coincidan con los requisitos de la base de datos externa. Después de modificar el archivo, ejecute las sentencias en la base de datos externa para crear las tablas de destino.
4. El canal de información externo debería estar ahora disponible para su uso en procesos de flujo de trabajo definidos a través del creador de procesos de auditoría. Consulte la documentación de Canal de información externo opcional para obtener información adicional.

Tema principal: Informes
Conceptos relacionados:
Canal de información externo opcional

Creador de informes distribuidos

Esta característica Gestor central proporciona una forma de recopilar automáticamente datos de todas las unidades gestionadas de Guardium o de un subconjunto de las mismas que están asociadas con este Gestor central. Los informes distribuidos están diseñados para proporcionar una vista de alto nivel, para correlacionar datos de orígenes de datos y, para resumir vistas de los datos. Continuaría utilizando agregadores para la recopilación de datos a nivel de fila entre los recopiladores.

Esta prestación alivia un problema que puede surgir en entornos empresariales complejos cuando los usuarios no siempre conocen la unidad gestionada exacta que tiene los datos necesarios para un informe en particular. Esto puede suceder porque el enlace entre los recopiladores y las bases de datos de Guardium puede cambiar con el tiempo que se basa en opciones de configuración como, por ejemplo, el equilibrio de carga. Esto se complica aún más por consideraciones como, por ejemplo, el periodo de tiempo y la política de retención de datos en el agregador y los recopiladores.

Es fácil crear un informe distribuido. Simplemente defínalo en la pantalla Informe distribuido, añádalo a un panel y estará listo para su uso.

Además, esta característica hace uso opcional de las despensas de datos en el Gestor central para habilitar la recopilación planificada de datos agregados a lo largo del tiempo. En esencia, los datos de informes distribuidos se almacenan en el Gestor central como una tabla sin formato, por lo que no son necesarias uniones complejas para crear el informe que desea, lo que puede mejorar significativamente el tiempo de respuesta para estos informes empresariales.

Los datos de informes distribuidos se pueden recopilar a partir de los Recopiladores, los Agregadores e incluso los Gestores centrales. Las versiones distribuidas predeterminadas de los informes incluyen el nombre de host de la unidad responsable de esos datos.

A continuación se muestran los informes distribuidos predefinidos:

- Verificación S-TAP de empresa
- Registro de agregación/archivado
- Intentos de inicio de sesión de usuario fallidos
- Excepciones de trabajos planificados

Ejecución de informes distribuidos: Inmediata o planificada

Cuando se define un informe distribuido, ejecútelo inmediatamente o planifique el informe para que se ejecute en segundo plano y recopile los resultados en el Gestor central:

- Inmediata: Esta modalidad recopila datos a petición (cuando se ejecute a través de la interfaz gráfica de usuario) y muestra los resultados al mismo tiempo que se recopilan los resultados de las unidades gestionadas relevantes. El informe distribuido incluye un indicador de estado de que los datos siguen en tránsito o que se han recibido todos los datos de una unidad gestionada determinada. En esta modalidad, los datos no se guardan en el Gestor central. Tan pronto como se cierre el informe, los datos se habrán perdido.
- Planificada: Esta modalidad recopila los datos por adelantado para habilitar la respuesta instantánea. En el intervalo de tiempo que especifique en el planificador, todos los datos relevantes agregados de las unidades gestionadas especificadas se envían a una tabla de despensa de datos designada en la máquina de Gestor central y crea un informe predeterminado en esta tabla. Esta tabla también tiene su propio dominio y entidad para habilitar la creación de informes y consultas adicionales utilizando el creador de consultas. Estos informes se pueden añadir a un proceso de auditoría para ejecutar el proceso de forma periódica y asignar los resultados del proceso a un Rol, Usuario y/o Grupo de usuarios para su revisión o validación.

Consideraciones de planificación para informes distribuidos

- En un entorno mixto donde el Gestor central es de 32 bits y las unidades gestionadas son de 64 bits, el Informe distribuido no mostrará información de los sistemas de 64 bits. Para ver información en esta situación, el Gestor central se tiene que actualizar a 64 bits.
- Debido a la coordinación de los datos que deben enviarse al Gestor central, es muy importante que la hora del reloj en todas las unidades gestionadas se establezca en la zona horaria en el huso horario en el que se encuentran las unidades gestionadas. Incluso una diferencia de diez minutos entre el Gestor central y las unidades gestionadas influye en el rendimiento y la fiabilidad de los informes distribuidos.
- Las definiciones de informe distribuidas planificadas se pueden exportar e importar, sin embargo, las definiciones de informes distribuidos inmediatas no se pueden exportar ni importar. La planificación propiamente dicha no se incluye en la definición importada ni exportada. Es recomendable que conserve un registro de las definiciones y la planificación si es necesario para volver a crearlo en otro sistema, como por ejemplo una copia de seguridad o prueba del Gestor central. Las copias de seguridad del sistema incluyen configuraciones de informes distribuidos.
- Si especifica que los datos de informe se recopilan de agregadores y recopiladores, es concebible que el informe distribuido predeterminado incluya datos duplicados (aunque el nombre de host de Guardium sea diferente). En este caso, es mejor especificar sólo los recopiladores o sólo los agregadores para la configuración de informes distribuidos.

- Los informes distribuidos se basan en informes existentes no distribuidos. Cuando se define un informe distribuido en modalidad planificada, si la consulta original incluye parámetros de tiempo de ejecución, se le solicitará que proporcione esos valores (o comodines, %).
- Planifique el hecho de que ahora tendrá datos que residen en el Gestor central en una base de datos que no había antes. Por lo tanto, tendrá que planificar los cambios operativos para la depuración, para las actualizaciones y para la copia de seguridad.

Creación de un informe distribuido

La creación de informes distribuidos sólo está disponible desde un dispositivo configurado como un Gestor central. Para acceder al creador de informes distribuidos al iniciar sesión como administrador, vaya a Informes > Herramientas de configuración de informes > Creador de informes distribuidos.

En el Creador de informes distribuidos, puede seleccionar en una lista de informes existentes para modificar la configuración o añadir a un panel, o pulse Nuevo para crear un informe distribuido nuevo. En general, cualquier informe existente en el Gestor central se puede distribuir inmediatamente o ejecutar en una planificación (o ambas).

Creación de un informe distribuido

En el Creador de informes, seleccione Nuevo, que borra los datos existentes en el creador de informes, en el desplegable Basado en informe, seleccione uno de los informes existentes que estén disponibles para su distribución. Cada informe de la lista se puede distribuir una vez como inmediato y una vez como planificado. Aquéllos que están definidos para distribuirse inmediatamente tienen el término (Immediate) añadido al nombre de informe distribuido.

Seleccione un informe existente para crear un informe distribuido.

En la sección Recopilar datos desde del constructor, seleccione Todas las unidades gestionadas (que gestiona el Gestor central) o especifique determinados grupos y/o unidades gestionadas específicas.

Nota: Puede definir grupos de unidades gestionados desde el Gestor central. Algunos ejemplos de grupos son: Grupo de recopiladores frente a agregadores; grupos que se basan en la aplicación, la responsabilidad o la geografía.

En la sección Modalidad de operación del creador, elija la modalidad de operación de informe:

- Inmediato: Ejecute el informe cuando el usuario lo solicite. Cuando se selecciona esta opción, no hay opciones adicionales a tener en cuenta. Puede pulsar en Aplicar para guardar los cambios y, a continuación, pulsar Añadir a panel para añadir el informe a la interfaz gráfica de usuario.
- Planificación: Se ejecuta en un proceso por lotes que prepara y reúne los datos de antemano.

Con la opción Informe planificado, puede especificar los valores adicionales siguientes:

- Granularidad de tiempo: Especifique el periodo de tiempo para el que se captura la Despensa de datos. La extracción de la Despensa de datos se realiza en el siguiente límite de intervalo de Granularidad de tiempo y cubre el intervalo de tiempo especificado. El extracto de la Despensa de datos para una granularidad de DAYS se inicia a medianoche y se ejecuta cada X días. El extracto de la Despensa de datos para una granularidad HOURS se inicia en el límite de la hora siguiente y se ejecuta cada X horas. El extracto de la Despensa de datos para una granularidad MINUTES se inicia en el siguiente límite de X minutos y se ejecuta cada X minutos. Por ejemplo, si especifica una Granularidad de tiempo de 1 hora para el informe Recuento de inicios de sesión fallidos, el recuento se basará en una agregación por hora de inicios de sesión fallidos.
- Depurar después: Especifique cuánto tiempo se deben mantener los datos de informe en la despensa de datos antes de que se depuren automáticamente.
- Parámetros de ejecución: En función del informe en el que esté basando el informe distribuido, debe especificar los parámetros de tiempo de ejecución. Para ver los valores válidos para estos campos, examine la consulta para el informe original o especifique el carácter comodín, %.

Pulse Aplicar. Cuando el sistema haya terminado de guardar la configuración de informe distribuido, se activan Modificar planificación y Roles.

Para crear la planificación, pulse Modificar planificación, que le lleva al planificador de propósito general.

La definición de planificación se envía a las unidades gestionadas e indica a cada unidad gestionada cuándo y con qué frecuencia deben enviarse los datos agregados al Gestor central.

Para especificar qué roles pueden ver este informe distribuido, pulse Roles.

Modificación de un informe distribuido existente

Para los informes distribuidos existentes, puede:

- Cambiar la configuración, incluidas las unidades gestionadas, los detalles de la planificación o los parámetros de tiempo de ejecución
- Añadir un informe a un panel de control
- Suprimir un informe distribuido
- Cree un informe planificado que se base en un informe inmediato existente. Esta opción sustituye el informe inmediato. No puede crear un informe inmediato a partir de un informe planificado existente.

Para seleccionar un informe existente, utilice el recuadro de búsqueda de texto o desplácese a través de la lista de informes existentes y seleccione el que desea modificar.

Visualización de informes distribuidos

Las siguientes columnas adicionales se incluyen en informes distribuidos:

- Fuente: El sistema de Guardium desde el que se han recopilado los datos.
- TZ: Huso horario-porque es posible que el sistema Guardium esté ubicado en un huso horario diferente del del Gestor central.
- Fecha: Esta columna muestra la hora del periodo de inicio para los informes planificados y para habilitar los resultados de acuerdo con hora/día. Para la modalidad Inmediata, esta columna muestra la hora de inicio y no será significativa.
  Nota: Sólo se permite un máximo de tres campos de fecha.

Editar y actualizar

Para informes distribuidos, edite y actualice el informe base y actualice el informe distribuido basándose en la estructura de informe actualizada.

Si un usuario cambia las columnas de un informe base, añade o elimina la cláusula where en el informe base y, a continuación, guarda y vuelve a generar el informe, a continuación, para actualizar el informe distribuido basado en este informe actualizado, el usuario sólo tiene que pulsar "Guardar cambios de informe" en el informe distribuido existente para que los cambios entren en vigor.

Si el usuario opta por actualizar el parámetro de informe existente, el usuario primero debe pulsar "Aplicar cambios de informe", a continuación, actualizar el valor de parámetro y, a continuación, pulsar "Guardar cambios de informe" para que las actualizaciones entren en vigor.

Más información sobre la hora

Cuando se ejecuta un informe, el personalizador de informes le permite especificar una ventana de tiempo absoluto para la consulta (de 3-31-2014 8:00am a 3-31-2014 11:00am) o una ventana de tiempo relativo (NOW -3 HOUR).

Para el tiempo absoluto, cada sistema Guardium se ejecutará en su hora local. Por ejemplo, si un informe distribuido recopila datos de sistemas Guardium en Horario Estándar del Este de EE.UU. (EST) y en Hora estándar del Pacífico (PST), cada sistema ejecutará la consulta en función de la hora local. En el ejemplo (útil para comprobar las horas punta, medianoche o cualquier hora absoluta específica), un sistema de Nueva York recopilará los resultados de 08:00 a 11:00 EST y un sistema en California reunirá los resultados de las 08:00 a las 11:00 PST.

Para una especificación de hora relativa, cada sistema ejecutará NOW -N de acuerdo con la hora actual en dicho sistema. Esto es importante para informes en tiempo real. No se puede utilizar el Tiempo absoluto para los informes en tiempo real o casi en tiempo real. Utilice la Modalidad inmediata para la supervisión en tiempo real.

Ver estado de informe distribuido

Cada informe distribuido va acompañado de un informe de estado que muestra al usuario las máquinas que proporcionan resultados y las que no. El enlace para acceder al informe de estado se resalta cuando se navega hasta el informe en la interfaz gráfica de usuario.

Para los informes planificados, al pulsar en una línea del Informe de estado se permite la ejecución de la API para volver a ejecutar el informe en la unidad o unidades específicas.

Si la ejecución específica para Informe distribuido en Modalidad planificada vuelve con un error, puede volver a ejecutar el informe desde el informe de estado de la siguiente manera:

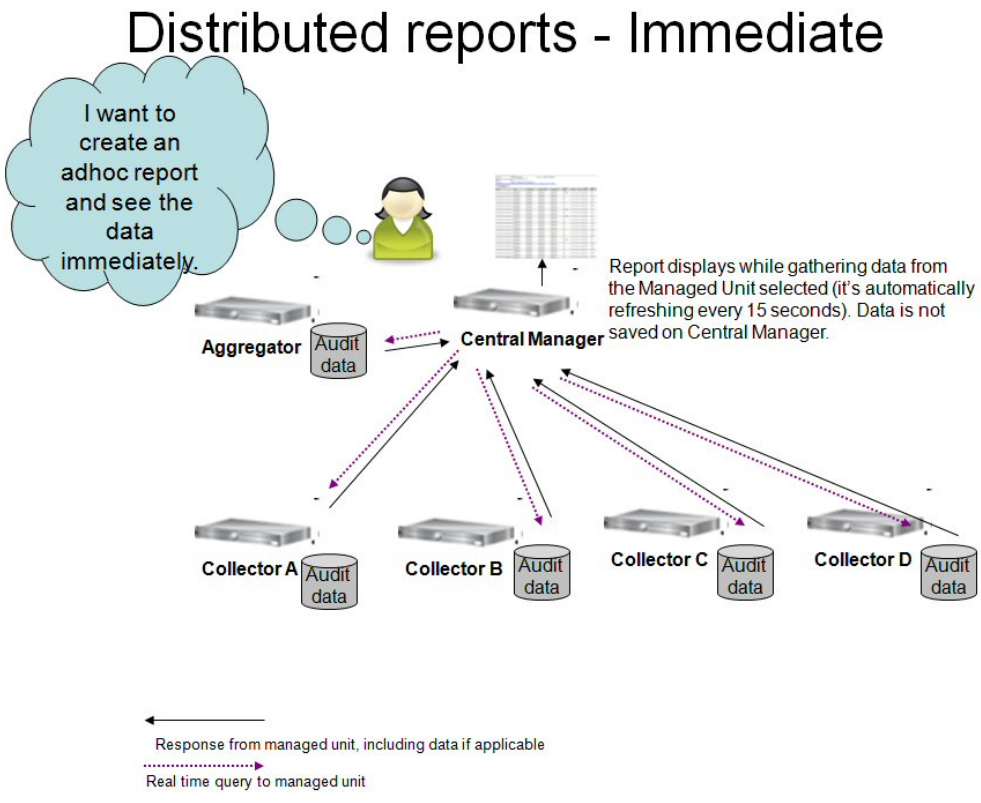
1. Efectúe una doble pulsación en una de las filas del informe de estado para que aparezca el menú Invocar. Pulse Invocar.
2. Pulse la selección, rerun_distributed_report.
3. Esto abrirá una pantalla emergente que le permite elegir la ejecución específica que se debe volver a ejecutar. Se puede abrir cualquier fila del informe, pero sólo se pueden volver a ejecutar las filas cuyo estado sea ERROR.

GuardAPI para volver a ejecutar el informe distribuido

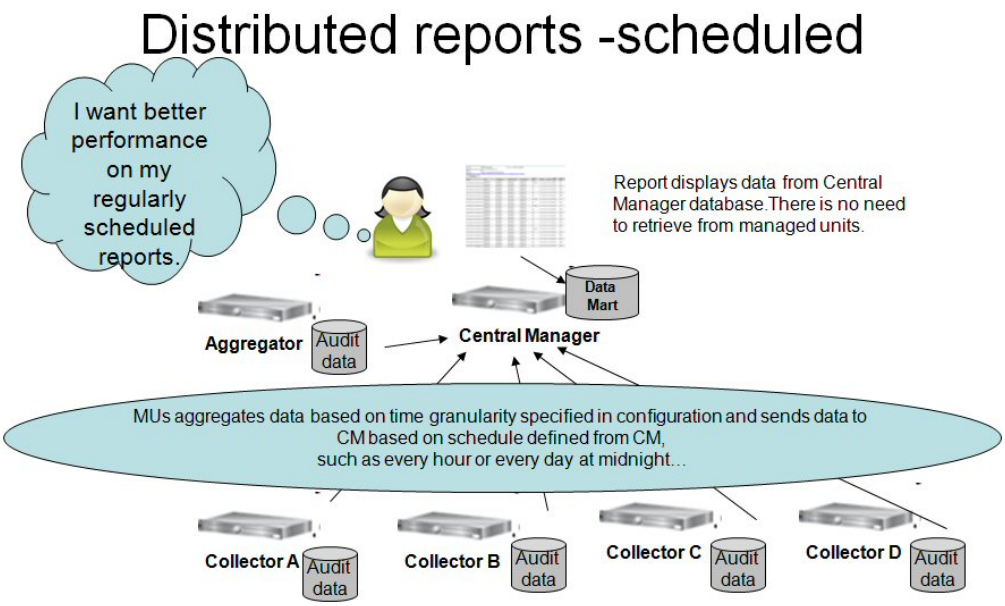
También se puede acceder al mandato de reintento descrito en la interfaz gráfica de usuario, para invocar el informe de estado, a través del mandato GuardAPI.

Sintaxis

grdapi rerun_distributed_report



Este diagrama ilustra el proceso para ejecutar un Informe distribuido inmediato.



Este diagrama ilustra el proceso para planificar un Informe distribuido.

Mejora de informe distribuido - establecer el sistema de destino en cualquier sistema Guardium

El Informe distribuido distribuye la solicitud de consulta en los sistemas Guardium especificados, recopila los datos en el Sistema de destino, consolida los resultados y proporciona vistas en los resultados consolidados. Los resultados están disponibles a través del Creador de consultas para la definición de consultas adicionales.

La característica Informe distribuido ahora puede establecer el sistema de destino en cualquier sistema de Guardium. La versión anterior no permite establecer el sistema de destino y siempre va al Gestor central (CM).

Justificación de requisito

En muchos casos, el CM está sobrecargado (independientemente del Informe distribuido) y el CM se utiliza en algún momento como un Agregador que añade carga al CM.

En estos casos, será mucho más eficaz permitir al usuario determinar el sistema de destino.

Solución

- Se puede establecer un Sistema de destino para cada Informe distribuido. Está disponible un mandato de CLI para establecer los sistemas de Destino opcionales. La lista establecida a través de la CLI se muestra en la interfaz gráfica de usuario del creador de Informes distribuidos.
- Nota importante: Este cambio sólo afecta a la modalidad Planificada de Informe distribuido. La modalidad Inmediata no está incluida en este cambio. Esto significa que sólo se puede acceder al visor de resultados de informes distribuidos ad-hoc a través del CM.
- La definición de Informe distribuido seguirá siendo editable sólo a través de CM.

Cambio de interfaz gráfica de usuario

- Se añade un nuevo campo "Enviar datos a" a la pantalla del Creador de informes distribuidos para permitir que el usuario establezca el/los Sistema(s) de destino (Recopilador(es) o Agregador(es)) para el Informe distribuido.
- Este campo sólo es relevante en el caso de la Modalidad planificada (de lo contrario, está inhabilitado).
- El valor predeterminado se establece en el CM.
- La lista de Sistemas de destino está limitada a los Sistemas que se han establecido a través de la CLI (consulte la lista de CLI más abajo).
- La definición de Informe distribuido se puede editar a través del CM y Ver sólo a través del destino.
- "Añadir a panel" del informe (adición del visor de informes al menú) está disponible en la pantalla de definición en el Sistema de destino y CM.
- Esta opción está disponible en CM incluso si el CM no es el Sistema de destino para dicho informe. Se ha hecho para dar la posibilidad de ver el Estado de informe distribuido en CM, pero no se mostrarán datos en el propio informe.

Los mandatos de CLI (sólo disponibles a través de la CM)

1. Establecer el sistema como un sistema de destino

grdapi set_distributed_report_target target_host_name=[nombre de host de unidad]

2. Cancelar el Sistema para que sea un Sistema de destino

grdapi cancel_distributed_report_target target_host_name=[nombre de host de unidad]

Si todavía hay informes distribuidos con esta unidad como destino, devuelve un error y la lista de informes de este tipo

3. Obtener lista de Sistemas de destino

grdapi get_distributed_report_target_info

Mandatos adicionales de CLI

Para informes de distribución planificados, almacenar o mostrar el valor de un número máximo de filas por unidad.

show scheduled_distributed

store scheduled_distributed

El Mandato de almacenamiento tiene un parámetro, maximum_rows_per_unit. Si el valor de dicho parámetro es mayor que 15.000 o es igual a 0 (sin límite), el usuario verá un mensaje de aviso:

"Dependiendo del número de recopiladores, establecer el número máximo de filas por unidad en un valor alto puede tener un impacto negativo en el rendimiento".

Tema principal: Informes

Cómo crear un Informe distribuido

Guardium ofrece una función que proporciona una forma de recopilar datos automáticamente de todas las unidades gestionadas de Guardium o de un subconjunto de unidades que están asociadas con un Gestor central de Guardium.

Acerca de esta tarea - En este ejemplo, vemos cómo obtener una vista más amplia y una visión de correlación para las excepciones (por ejemplo, errores de SQL) que se registran en recopiladores específicos.

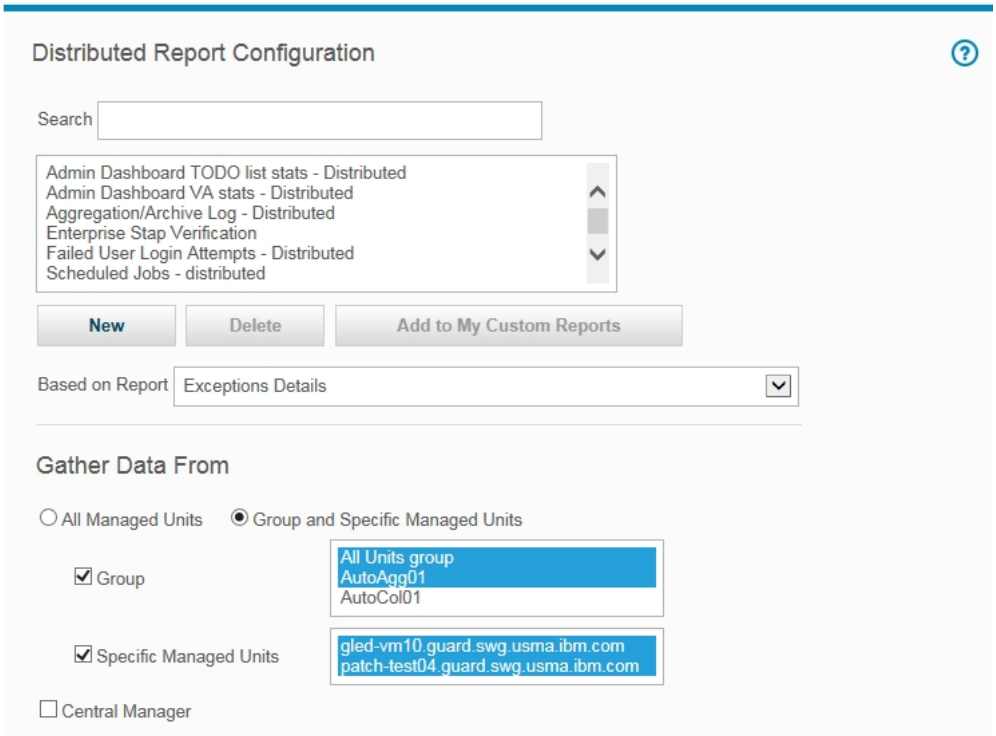
Resumen de pasos

Requisitos previos - Crear grupo de Unidades gestionadas a través de la pantalla Gestión central.

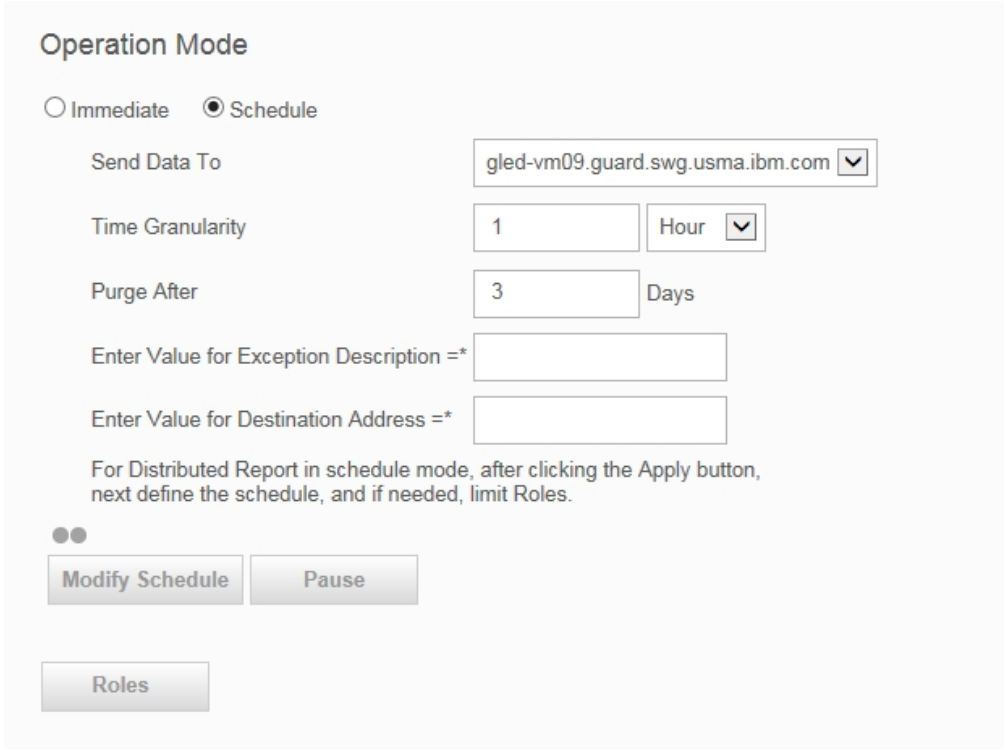
1. Cree un Informe distribuido.
2. Revise los datos recopilados.
3. Cree informes de resumen adicionales en los datos recopilados.

Procedimiento

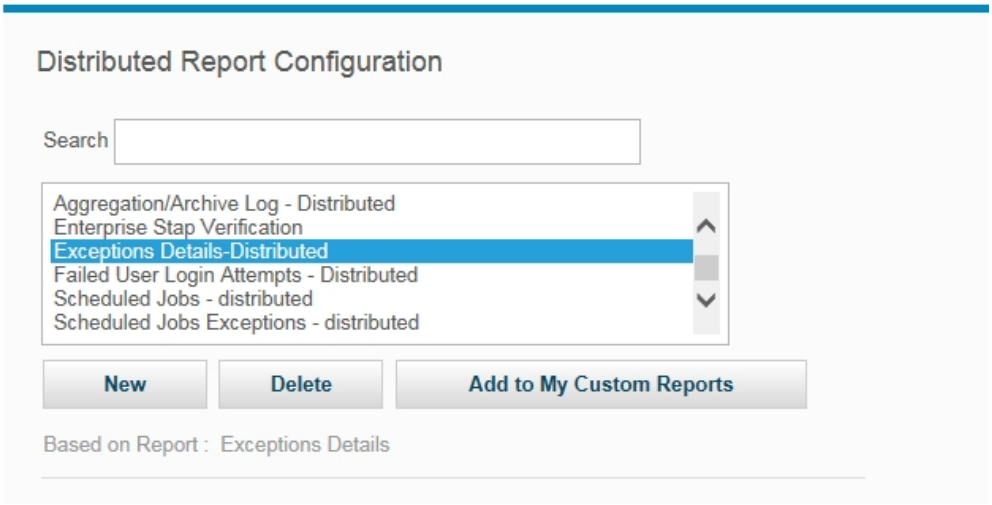
1. Pulse Informes > Herramientas de configuración de informes > Creador de informes distribuidos.
2. Pulse Nuevo.
3. Seleccione Basado en informe en la lista (la lista muestra los Informes definidos por el usuario). Para este ejemplo, seleccione Detalles de excepciones.



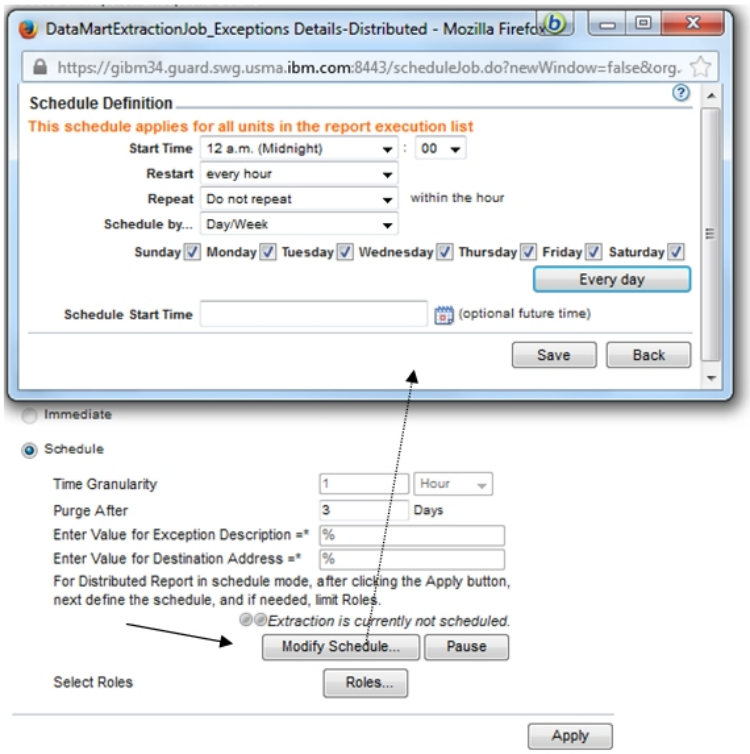
4. Mueva la pantalla hacia abajo para especificar las Unidades gestionadas que se deben incluir en este informe distribuido. Para este ejemplo, elija dos grupos de la lista Grupo y, además, unas pocas unidades gestionadas en la lista Unidades gestionadas. En este ejemplo, deje deseleccionado el 'Gestor central' (en el caso de que el Gestor central también sea un Agregador, es posible que se tenga que incluir).
5. La siguiente captura de pantalla muestra el valor para la Modalidad de funcionamiento. La modalidad Inmediata es principalmente para la supervisión en línea/en tiempo real como, por ejemplo, ver los Intentos de inicio de sesión fallidos, ver las Excepciones excesivas recientes o ver las alertas en tiempo real. La modalidad Planificada es una recopilación de datos en curso que se ejecuta periódicamente en función de la Planificación definida. Este ejemplo resume las excepciones cada hora. Existe un requisito para cumplimentar valores para Descripción de excepción y Dirección de destino.



6. Pulse Aplicar para crear el Informe distribuido.
7. Una vez aplicado, el nuevo Informe distribuido se añade y se resalta en el recuadro de lista.

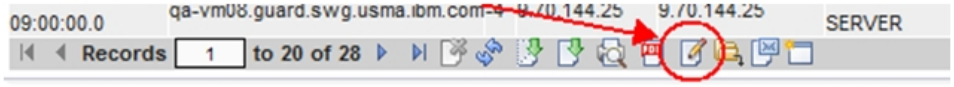


8. El paso siguiente es planificarlo pulsando Modificar planificación (es obligatorio para activar el proceso).



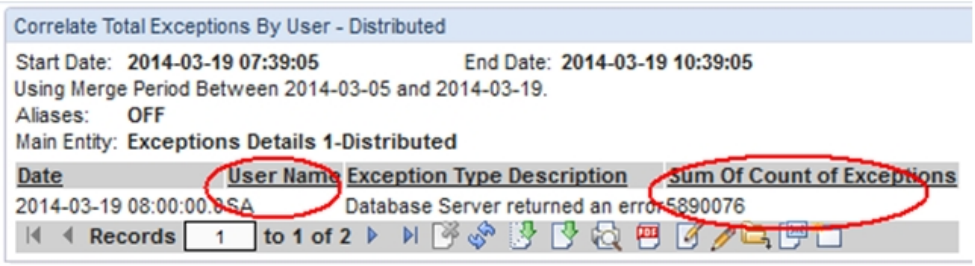
9. Este informe se puede limitar a roles específicos pulsando Roles y seleccionando los Roles pertinentes.
10. En este ejemplo específico, el informe se realiza cada hora: no hay necesidad de esperar al menos una hora para obtener los resultados iniciales.
    Nota: La línea que dice 'Estado de informe distribuido - pulse aquí para obtener detalles', muestra el estado de la recopilación de datos; si faltan datos en las unidades gestionadas, la línea aparece de color rojo; al pulsar en la línea se navega hasta el informe de detalles de estado por unidades por hora.

11. Los datos se recopilan de todas las Unidades gestionadas especificadas y se almacenan en una entidad (tabla) designada nueva. Esta entidad ahora está disponible a través del Creador de consultas y del Creador de informes para crear Consultas e Informes adicionales en esta nueva tabla. La opción de crear Consultas e Informes adicionales también está disponible a través de la pantalla de resultados Informe distribuido. Pulse Editar la consulta para este informe.



    Este Informe predeterminado no se puede modificar; pulse Clonar, póngale un nombre, elimine todos los atributos y deje la Fecha, Nombre de usuario, Descripción del tipo de excepción, y la Suma de recuento de excepciones.

La siguiente captura de pantalla muestra un ejemplo de las Excepciones totales de correlación por usuario (Distribuido). Esta vista suma las excepciones totales por usuario de todas las bases de datos que están asociadas a las Unidades gestionadas de Guardium seleccionadas para este Informe distribuido. Asimismo, puede ver el Total de intentos de inicio de sesión fallidos en todo el sistema, o el Total de excepciones por programas de origen.



Tema principal: Informes

Asesorar y reforzar

La solución de asesoramiento de vulnerabilidades de Guardium es el primer paso en la gestión del ciclo de vida de seguridad y conformidad para cualquier entorno TI. Puede utilizar un conjunto de asesoramientos predefinidos o personalizados y procesar auditorías de flujo de trabajo para identificar y direccionar vulnerabilidades de base de datos de forma automática, mejorando de forma proactiva las configuraciones y reforzando infraestructuras.

- Inicio al asesoramiento de vulnerabilidades de Guardium
  Asesoramiento de vulnerabilidades de Guardium le permite identificar y corregir vulnerabilidades en la infraestructura de la base de datos.
- Pruebas de asesoramiento de vulnerabilidades
  Guardium proporciona varios tipos de pruebas que le permiten evaluar la vulnerabilidad.
- Asesoramientos
  Los asesoramientos son un grupo de pruebas que escanean las infraestructuras de base de datos en busca de vulnerabilidades y proporcionan una evaluación de la salud de seguridad de la base de datos y de los datos con medidas históricas y en tiempo real.
- Cambio de esquema necesario
  El esquema que han utilizado las pruebas de asesoramiento de vulnerabilidades en IBM DB2 for z/OS ha cambiado en Guardium V9.1. Si actualiza de una versión anterior a 9.1, deberá actualizar la base de datos para poder continuar utilizando estas pruebas.
- Asesoramiento de vulnerabilidades de RACF
  Si utiliza IBM DB2 for z/OS, puede utilizar pruebas de asesoramiento de vulnerabilidades para asesorar las vulnerabilidades de RACF. Debe tener al menos la versión 9.1 de Guardium instalada para utilizar los asesoramientos de RACF.
- CAS (Configuration Auditing System)
  CAS realiza un seguimiento de dichos cambios e informes en ellos. Los datos están disponibles en el sistema Guardium y se puede utilizar para informes y alertas.

Inicio al asesoramiento de vulnerabilidades de Guardium

Asesoramiento de vulnerabilidades de Guardium le permite identificar y corregir vulnerabilidades en la infraestructura de la base de datos.

El asesoramiento de vulnerabilidades de base de datos escanea la infraestructura de base de datos para detectar vulnerabilidades y proporcionar la evaluación del estado de la base de datos y la seguridad de datos, con medidas históricas y en tiempo real.

El asesoramiento de vulnerabilidades utiliza tres tipos de artefactos:

Prueba
: Una prueba comprueba el entorno de base de datos de vulnerabilidades de una amenaza o un área de interés concretas.

Asesoramiento
: Un asesoramiento es un trabajo que incluye un conjunto de pruebas que se ejecutan conjuntamente.

Origen de datos
: El mismo origen de datos como, por ejemplo, una base de datos o un archivo XML, y la información de conexión necesaria para acceder a los datos.

La aplicación Asesoramiento de vulnerabilidades de Guardium habilita organizaciones para identificar y direccionar vulnerabilidades de bases de datos de forma coherente y automatizada. El proceso de asesoramiento de Guardium evalúa el estado de los entornos de base de datos y le recomienda mejorar:

- La evaluación de la configuración del sistema frente a las prácticas recomendadas y la búsqueda de vulnerabilidades o amenazas potenciales en los recursos de base de datos, incluidos los riegos de configuración y de comportamiento. Por ejemplo, la identificación de todas las cuentas predeterminadas que no se han inhabilitado; la comprobación de los privilegios públicos y los métodos de autenticación seleccionados, etc.
- La búsqueda de vulnerabilidades inherentes presentes en el entorno TI, como los parches de seguridad que faltan,
- La recomendación y priorización de un plan de acción basado en áreas descubiertas de los riesgos y vulnerabilidades más críticos. La generación de informes y recomendaciones proporciona directrices acerca de cómo realizar cambios de conformidad y elevar la seguridad del entorno de base de datos evaluado

El asesoramiento de vulnerabilidades de base de datos de Guardium combina dos métodos de prueba esenciales para garantizar la amplitud y profundidad de cobertura. Aprovecha varias fuentes de información para recopilar una imagen completa del estado de seguridad de la base de datos y del entorno de datos.

1. Basado en agente: Utilización de software instalado en cada punto final (p. ej. servidor de base de datos). Pueden determinar aspectos de cada punto final que no se pueden determinar de forma remota como, por ejemplo, el acceso del administrador a datos confidenciales directamente desde la consola de base de datos.
2. Escaneo: Interrogación y punto final en la red mediante el acceso con credenciales.

Se incluyen en la solución de vulnerabilidades y gestión de amenazas de Guardium:

- El descubrimiento automático de base de datos realiza un descubrimiento automático de red del entorno de base de datos y crea una representación gráfica de las interacciones entre servidores y clientes de base de datos.
- El clasificador de contenido de base de datos descubre y clasifica de manera automática datos confidenciales como, por ejemplo, números de tarjetas de crédito de 16 dígitos y números de la seguridad social de 9 dígitos, y ayuda a las organizaciones a identificar rápidamente procesos empresariales o de TI defectuosos que almacenan datos confidenciales.
- El asesoramiento de vulnerabilidades de base de datos explora la infraestructura de base de datos para detectar vulnerabilidades y proporciona la evaluación del estado de la base de datos y de la seguridad de datos, con medidas históricas y en tiempo real.
- CAS (Configuration Auditing System) realiza un seguimiento de todos los cambios realizados en elementos como las estructuras de base de datos, controles de seguridad y de acceso, valores de datos críticos y archivos de configuración de base de datos.
- La automatización de flujo de trabajo de cumplimiento automatiza todo el proceso de conformidad empezando por el asesoramiento y el refuerzo, la supervisión de actividades para la creación de informes de auditoría, la distribución de informes y la aprobación por parte de las partes interesadas de clave.

CAS (Configuration Auditing System) desempeña un rol importante en la identificación de vulnerabilidades y amenazas. Las plantillas de CAS definidas por el usuario y preconfiguradas de Guardium pueden utilizarse en la prueba de asesoramiento y aportar así una vista holística del entorno de base de datos del cliente; con CAS, Guardium puede identificar vulnerabilidades de la base de datos a nivel de SO como, por ejemplo, permisos de archivo, propiedad y variables de entorno. Estas pruebas se pueden ver a través del panel Definición del conjunto de plantillas de CAS y tienen la palabra *asesoramiento* en su nombre.

Nota: Solo se ofrece soporte al asesoramiento de vulnerabilidades (VA) y a CAS (Configuration Auditing System) en inglés.

Common Vulnerabilities and Exposures (CVE®) es un diccionario de nombre comunes (p.ej., identificadores CVE) de vulnerabilidades de seguridad de la información conocidas públicamente. Los identificadores comunes de CVE facilitan la compartición de datos entre herramientas y bases de datos de seguridad de red, y proporcionan una línea base para evaluar la cobertura de tal modo que, si un informe incorpora identificadores CVE, los usuarios pueden acceder de forma rápida y precisa a la información del arreglo en una o más bases de datos compatibles con CVE para solucionar el problema.

Numerosas organizaciones han hecho que sus productos y servicios de seguridad de información sean compatibles con CVE al incorporar identificadores CVE. Guardium supervisa constantemente las vulnerabilidades y exposiciones comunes (CVE) de MITRE Coporation y añade estas pruebas para las vulnerabilidades relacionadas con la

base de datos relevante.

Al configurar pruebas mediante el Creador de asesoramientos de seguridad, el usuario puede seleccionar el botón de selección de CVE para la base de datos deseada y, a continuación, seleccionar y añadir el identificador de CVE apropiado para ayudar en la búsqueda de vulnerabilidades individuales mientras se visualizan los nombres de CVE de bases de datos específicas. Encontrará información adicional en la copia maestra de la lista de CVE que mantiene MITRE Corporation.

Para mantener las CVE actuales en la solución Guardium, este descargará y utilizará la base de datos de CVE más actual para completar una tabla de base de datos con todas las entradas y candidatos de CVE actuales.Guardium compara mediante programación los datos de CVE descargados con los datos de CVE que se encuentran en el repositorio de asesoramiento de vulnerabilidades de Guardium, generando una lista de CVE nuevos para revisar. A continuación, el equipo de seguridad de bases de datos de Guardium revisará manualmente los candidatos para base de conocimiento de vulnerabilidad de Guardium, los probará y añadirá los relevantes en el equipo de seguridad de asesoramientos de vulnerabilidades de Guardium. Estas pruebas se etiquetan con el número de CVE apropiado, y una vez en el repositorio GA, se pueden ejecutar automáticamente utilizando la aplicación Asesoramiento de vulnerabilidades de Guardium.

Nota:

- Tanto en los asesoramientos de vulnerabilidades como en los informes de titularidad, cuando busque scripts para otorgar privilegios a los informes de titularidad, utilice los scripts del directorio gdmmonitor_scripts. No utilice la carpeta entitlement_monitor_role, que ya no se actualiza.
- Al utilizar una clave de licencia de un producto con caducidad, o una licencia con un número limitado de orígenes de datos, aparece el mensaje siguiente: `No se puede añadir el origen de datos. Se ha alcanzado el número máximo de orígenes de datos permitido por la licencia.` La fecha Licencia válida hasta y Número de orígenes de datos se pueden visualizar en el panel Configuración del sistema de la Consola de administrador. Los procesos de clasificación o de vulnerabilidad con orígenes de datos *N* se cuentan como escaneos *N* cada vez que se ejecutan.
- Los asesoramientos de vulnerabilidades de Guardium requieren acceso a las bases de datos que evalúan. Para ello, Guardium proporciona un conjunto de scripts SQL (un script para cada tipo de base de datos) que crean usuarios y roles en la base de datos que va a utilizar.

  Los scripts de plantilla están disponibles en el sistema Guardium cuando este se haya creado, y se pueden encontrar y descargar mediante un servidor de archivos en la siguiente vía de acceso: /log/debug-logs/gdmmonitor_scripts/. Encontrará más información en el archivo README.txt.

Excepciones de pruebas de asesoramiento de vulnerabilidades de Guardium

Los grupos de excepciones de pruebas de asesoramiento de vulnerabilidades de Guardium se cumplimentan de forma previa con los privilegios, objetos, esquemas o miembros predeterminados creados cuando se instala una base de datos. Utilice estos grupos para evitar falsos positivos cuando se ejecuten los asesoramientos de vulnerabilidades. Si el asesoramiento falla, enlace el grupo de excepciones apropiado para la prueba para excluir los miembros predeterminados y ejecutar la prueba de nuevo: si la prueba ahora se ejecuta sin infracciones, indicará que las infracciones iniciales se debían a los privilegios, objetos, esquemas o miembros creados al instalar la base de datos.

Tabla 1. Grupos de asesoramiento de vulnerabilidades para probar la correlación

ID de grupo	Nombre de grupo	Nombre de la prueba	ID de prueba	Tipo de base de datos
82	Sybase Allowed Grants to Public	Sin privilegios públicos no exentos	61	SYBASE ASE
83	MS-SQL Allowed Grants to Public	Sin privilegios públicos no exentos	270	MSSQL
115	DB2 Allowed Grants to Public	Sin privilegios de objetos públicos	105	DB2 LUW
144	DB2 Allowed Grants to Public non-restrictive	Sin privilegios de objetos públicos	105	DB2 LUW
116	Teradata Allowed Grants to Public	Privilegios de objeto otorgados a PUBLIC	2029	TERADATA
117	PostgreSQL Allowed Grants to Public	Privilegios de objetos otorgados a PUBLIC	315	POSTGRESQL
118	Netezza Allowed Grants to Public	Privilegios de objeto otorgados a PUBLIC (Netezza)	2053	NETEZZA
65	MS-SQL Database Administrators	Sólo los DBA en roles de servidor fijos	159	MSSQL
165	Oracle Only DBA Access To SYS.USER$	Sólo acceso DBA a SYS.USER$	222	ORACLE
166	MS-SQL DDL granted to user	DDL otorgado al usuario	321	MSSQL
167	MS-SQL Procedures granted to users	Procedimientos otorgados a los usuarios	322	MSSQL
168	MS-SQL No Individual User Privileges	Sin privilegios de usuarios individuales	154	MSSQL
170	Sybase IQ Procedures and functions granted to PUBLIC	Procedimientos y funciones otorgados a PUBLIC.	2230	SYBASE IQ
171	Sybase IQ No individual procedures or functions privileges	Sin privilegios de funciones o procedimientos individuales.	2227	SYBASE IQ
172	MS-SQL No Access to Registry Access Extended procedures	Sin acceso a procedimientos ampliados de acceso a registros	215	MSSQL
173	MS-SQL Role granted to role	Rol otorgado al rol	323	MSSQL
185	MS-SQL Access to server level permissions granted to non-Database Administrators	Acceso a permisos a nivel de servidor otorgados a usuarios que no son administradores de bases de datos	2289	MSSQL
186	MS-SQL MSDB database Role Members Privilege	Privilegio de miembros de rol de base de datos MSDB	2296	MSSQL

ID de grupo	Nombre de grupo	Nombre de la prueba	ID de prueba	Tipo de base de datos
48	DB2 Database Version+Patches	Versión: DB2	16	DB2 LUW
48	DB2 Database Version+Patches	Nivel de parche de DB2	54	DB2 LUW
49	Informix Database Version+Patches	Versión: Informix	17	INFORMIX
49	Informix Database Version+Patches	Nivel de parche de Informix	55	INFORMIX
50	MS Sql Server Database Version+Patches	Versión: Microsoft SQL Server	18	MSSQL
50	MS Sql Server Database Version+Patches	Nivel de parche de Microsoft SQL Server	56	MSSQL
51	MySql Database Version+Patches	Versión: MySql	19	MYSQL
51	MySql Database Version+Patches	Nivel de parche de MySql	57	MYSQL
52	Oracle Database Version+Patches	Nivel de parche de Oracle	58	ORACLE
52	Oracle Database Version+Patches	Versión: Oracle	20	ORACLE
53	Sybase Database Version+Patches	Versión: Sybase	21	SYBASE ASE
53	Sybase Database Version+Patches	Nivel de parche de Sybase	59	SYBASE ASE
109	Teradata PDE Version+Patches	Versión: Teradata PDE	284	TERADATA
109	Teradata PDE Version+Patches	Nivel de parche de Teradata PDE	286	TERADATA
110	Teradata TDBMS Version+Patches	Nivel de parche de Teradata TDBMS	287	TERADATA
110	Teradata TDBMS Version+Patches	Versión: Teradata TDBMS	285	TERADATA
111	Teradata TDGSS Version+Patches	Versión: Teradata TDGSS	290	TERADATA
111	Teradata TDGSS Version+Patches	Nivel de parche de Teradata TDGSS	288	TERADATA
112	Teradata TGTW Version+Patches	Versión: Teradata TGTW	291	TERADATA
112	Teradata TGTW Version+Patches	Nivel de parche de Teradata TGTW	289	TERADATA
113	Netezza Version+Patches	Nivel de versión de Netezza	306	NETEZZA
113	Netezza Version+Patches	Nivel de parche de Netezza	307	NETEZZA
114	Postgress Version+Patches	Nivel de versión de PostGreSQL	308	POSTGRESQL
114	Postgress Version+Patches	Nivel de parche de PostGreSQL	309	POSTGRESQL
169	SybaseIQ Database Version+Patches	Versión: Sybase IQ	377	SYBASE IQ
169	SybaseIQ Database Version+Patches	Nivel de parche de Sybase IQ	378	SYBASE IQ

MongoDB

Desarrollado en 2007, MongoDB es una base de datos NoSQL orientada a documentos. Utiliza documentos JSON con esquemas dinámicos (este formato se denomina BSON). En MongoDB, una recopilación es el equivalente a una tabla RDBMS, mientras que los documentos son equivalentes a los registros de una tabla RDBMS.

Se trata del sistema de base de datos NoSQL de mayor crecimiento y el más rápido. Tiende a utilizarse como sistema operativo y como programa de fondo para aplicaciones web debido a la facilidad de programación de datos con formato no relacionales como, por ejemplo, los documentos JSON que a menudo se encuentran en aplicaciones web.

- Primera base de datos NoSQL soportada para Asesoramiento de vulnerabilidades de Guardium (VA)
- Primera conexión de base de datos no JDBC. La conexión utiliza un controlador Java.
- Los orígenes de datos de MongoDB dan soporte a conexiones de servidor SSL y cliente/servidor con certificados de cliente de SSL.
- La solución de asesoramiento de vulnerabilidades de los clústeres de MongoDB se puede ejecutar en mongos, un nodo primario y todos los nodos secundarios para los conjuntos de réplicas.
- No se da soporte a los informes de titularidad y el creador basado en consultas en MongoDB.

Origen de datos MongoDB con SSL

Puede importar certificados de servidor que realizamos de manera más discreta para los autofirmados. El cliente también puede importar su certificado. Los certificados también funcionan en el gestor central y se envían a los recopiladores.

CAS para MongoDB

La plantilla de asesoramiento de CAS de Mongo permite especificar varias vías de acceso en el origen de datos para explorar diversos componentes del sistema de archivos.

Teradata Aster

Aster Data

Adquirido por Teradata en 2011, normalmente se utiliza para aplicaciones analíticas y de depósito de datos (OLAP). Aster Data creó una infraestructura denominada SQL-MapReduce que permite el uso de SQL (Structured Query Language) con Map Reduce. A menudo se asocia con tipos de secuencia de clics de aplicaciones.

Se debe crear un asesoramiento de seguridad para ejecutar todas las pruebas en el nodo queen, y todas las conexiones de base de datos de Aster Data pasan solo por dicho nodo.

Las pruebas en los nodos de trabajador y de cargador solo son necesarias cuando se realizan pruebas de CAS (permiso de archivo y propiedad de archivo).

Las pruebas de privilegios pasan por todas las bases de datos de una instancia determinada de Aster.

SAP HANA

SAP HANA es un sistema de gestión de bases de datos relacional, orientado en columnas y en la memoria desarrollado y comercializado por SAP SE. La arquitectura de HANA está diseñada para manejar velocidades altas de transacción y un proceso de consultas complejo en la misma plataforma.

- Privilegios de base de datos para clasificación y asesoramiento de vulnerabilidades
  Guardium proporciona un amplio conjunto de scripts para simplificar la creación de grupos o roles con los privilegios mínimos necesarios para ejecutar los asesoramientos de vulnerabilidades.
- Despliegue de asesoramiento de vulnerabilidades para DB2 para i
  Habilitar un grupo de usuarios para ejecutar asesoramientos de vulnerabilidades y configurar y ejecutar las pruebas.
- Utilización del asesoramiento de vulnerabilidades con Cloudera
  Aprenda a utilizar el asesoramiento de vulnerabilidades de Guardium con las distribuciones de Cloudera de Apache Hadoop.

Tema principal: Asesorar y reforzar

Privilegios de base de datos para clasificación y asesoramiento de vulnerabilidades

Guardium proporciona un amplio conjunto de scripts para simplificar la creación de grupos o roles con los privilegios mínimos necesarios para ejecutar los asesoramientos de vulnerabilidades.

Antes de empezar

Esta tarea requiere bajar scripts desde un sistema Guardium y ejecutarlos en un servidor de bases de datos. Necesitará identificar la dirección IP de la máquina que se utilizará para acceder al sistema de Guardium. Puede ser la dirección IP de una estación de trabajo individual donde bajará los scripts antes de transferirlos al servidor de bases de datos o puede ser la dirección IP del propio servidor de bases de datos.

Acerca de esta tarea

La ejecución de los asesoramientos de vulnerabilidades de Guardium y la utilización del clasificador de Guardium requiere acceso a la base de datos y privilegios específicos de base de datos. Guardium proporciona un amplio conjunto de scripts para simplificar la creación de grupos o roles con los privilegios mínimos necesarios para ejecutar los asesoramientos de vulnerabilidades.Una vez creados, estos grupos o roles se pueden asignar a cualquier usuario de base de datos que necesite ejecutar un asesoramiento. Creará un origen de datos de Guardium con este usuario para realizar el escaneo del asesoramiento de vulnerabilidades (VA).

Los scripts se proporcionan para dar soporte a la mayoría de los tipos de base de datos y están diseñados para ser ejecutados en la propia herramienta de base de datos. Cada script incluye instrucciones detalladas en su cabecera. Los privilegios otorgados para cada tipo de base de datos se pueden ver en los propios script en cada mandato de otorgamiento de permiso.
Importante: Antes de ejecutar ningún script, los administradores de base de datos deberían leer las instrucciones en las cabeceras de los scripts y revisar las acciones de base de datos que realizarán dichos scripts.

Procedimiento

1. En un sistema Guardium, habilite el servidor de archivos mediante el mandato de CLI fileserver. Por ejemplo, para habilitar el servidor de archivos durante una hora y bajar los scripts al sistema con la dirección IP `10.0.0.1`, utilice el siguiente mandato:

   ```
   fileserver 10.0.0.1 3600
   ```

   Una vez iniciado de forma satisfactoria, el servidor de archivos debería visualizar una salida similar a la siguiente:

   ```
   Iniciando el servidor de archivos...
   El servidor de archivos está listo en https://guardium.host.com:8445
   El tiempo de espera se ha establecido en 3600 segundos y se puede exceder
   durante la subida.

   La subida solo será accesible desde la dirección IP desde la que ha
   iniciado una sesión: 10.0.0.1

   Pulse Intro para detener el servidor de archivos.
   ```

2. En la máquina donde baje los archivos, utilice un navegador web para acceder al servidor de archivos. Por ejemplo, para un sistema de Guardium que se ejecuta en `https://guardium.host.com:8445`, acceda a los scripts para el asesoramiento de vulnerabilidades y clasificación en los siguientes URL:

   ```
   https://guardium.host.com:8445/log/debug-logs/gdmmonitor_scripts/
   https://guardium.host.com:8445/log/debug-logs/classification_role/
   ```

   Importante: Los procesos de descubrimiento del clasificador de Guardium precisan un mayor nivel de acceso a la base de datos que el necesario para las pruebas de asesoramientos de vulnerabilidades. Se recomienda utilizar los scripts en `gdmmonitor_scripts` para el asesoramiento de vulnerabilidades y los scripts en `classification_role` para el clasificador. Antes de ejecutar ningún script, los administradores de base de datos deberían leer las instrucciones en las cabeceras de los scripts y revisar las acciones de base de datos que realizarán dichos scripts. Antes de ejecutar ningún script, los administradores de base de datos deberían leer las instrucciones en las cabeceras de los scripts y revisar las acciones de base de datos que realizarán dichos scripts.
3. Baje los scripts necesarios utilizando la acción Pulsar con el botón derecho del ratón > Guardar enlace como... del navegador web o una funciona similar. Consulte los archivos README.txt para identificar los scripts correctos para utilizar con los tipos de base de datos específicos.
   Consejo: Hay tres scripts para Microsoft SQL Server:
   - gdmmonitor-mss2000-only.sql para Microsoft SQL Server 2000
   - gdmmonitor-mss.sql para Microsoft SQL Server 2005 y más reciente

- gdmmonitor-mss-SA.sql para proporcionar los privilegios administrativos necesarios para los seis tipos de asesoramiento de vulnerabilidades de Microsoft SQL Server. Si no permite estos privilegios, las pruebas devolverán errores que indicarán privilegios inadecuados. Estas seis pruebas representan no más del 5% de las pruebas disponibles.

Qué hacer a continuación

Una vez haya descargado los scripts necesarios para sus servidores de bases de datos, consúltelos con detalle y siga las instrucciones en las cabeceras de los scripts.

Tema principal: Inicio al asesoramiento de vulnerabilidades de Guardium

Despliegue de asesoramiento de vulnerabilidades para DB2 para i

Habilitar un grupo de usuarios para ejecutar asesoramientos de vulnerabilidades y configurar y ejecutar las pruebas.

Acerca de esta tarea

Pasos de despliegue

1. El asesoramiento de vulnerabilidades se despliega desde el sistema Guardium.
2. El usuario ejecuta un script proporcionado por Guardium en la base de datos de destino para crear un rol con los privilegios adecuados. A continuación, crea una conexión de origen de datos en la base de datos.
3. Cree un asesoramiento de vulnerabilidades y, a continuación, seleccione los orígenes de datos y las pruebas que desea ejecutar.
4. Cuando se haya realizado la ejecución, se crea un informe que muestra las pruebas que han pasado y/o fallado junto con las recomendaciones de protección.

Soporte de IBM para versión i:

IBM para i 6.1, 7.1 y 7.2

Cobertura de prueba de VA (115 pruebas en total):

Perfiles con autorizaciones especiales

Perfiles con acceso al uso de función de base de datos

Políticas de contraseña

Privilegio de objetos de base de datos concedidos a PUBLIC

Privilegios de objetos de base de datos concedidos a un usuario individual

Privilegios de objetos de base de datos concedidos con opción grant

APAR de seguridad

Informes de titularidad:

Perfiles con autorizaciones especiales

Grupo concedido al usuario

Privilegio de objetos de base de datos concedidos a PUBLIC

Privilegios de objetos ejecutables de base de datos concedidos a PUBLIC

Privilegios de objetos de base de datos concedidos a un usuario individual

Privilegios de objetos de base de datos concedidos con opción grant

Procedimiento

1. Utilice el Creador de grupos para crear un grupo de usuarios para el que desee utilizar el asesoramiento de vulnerabilidades. Abra el Creador de grupos pulsando Configuración > Herramientas y vista > Creador de grupos. El paso siguiente utiliza un script para un grupo denominado gdmmonitor.
2. Ejecute el script siguiente en el sistema i de DB2 para conceder los privilegios necesarios i ejecutar el asesoramiento de vulnerabilidades en el grupo. Esta acción se realiza fuera del sistema Guardium mediante un cliente nativo de base de datos.

```
grant select on SYSIBMADM.FUNCTION_INFO to gdmmonitor;
grant select on SYSIBMADM.FUNCTION_USAGE to gdmmonitor;
grant select on SYSIBMADM.GROUP_PROFILE_ENTRIES to gdmmonitor;
grant select on SYSIBMADM.SYSTEM_VALUE_INFO to gdmmonitor;
grant select on SYSIBMADM.USER_STORAGE to gdmmonitor;
grant select on Qsys2.Authorizations to gdmmonitor;
grant select on SYSIBMADM.USER_INFO to gdmmonitor;
grant select on QSYS2.SYSSCHEMAAUTH to gdmmonitor;
grant select on QSYS2.SYSTABAUTH to gdmmonitor;
grant select on QSYS2.SYSPACKAGEAUTH to gdmmonitor;
grant select on QSYS2.SYSROUTINEAUTH to gdmmonitor;
grant select on QSYS2.SYSSEQUENCEAUTH to gdmmonitor;
grant select on QSYS2.SYSCOLAUTH to gdmmonitor;
```

Para la IBM DB2 para i versión 7.1 y posterior, incluya también los scripts:

```
grant select on QSYS2.SYSVARIABLEAUTH to gdmmonitor;
grant select on QSYS2.SYSXSROBJECTAUTH to gdmmonitor;
```

3. Cree una conexión JDBC en DB2 para el sistema i. Abra Buscador de orígenes de datos pulsando Configuración > Herramientas y vistas > Definiciones de origen de datos, y luego seleccione Asesoramiento de seguridad del menú Selección de aplicaciones.
    a. Pulse Nuevo y especifique la información adecuada. Para Propiedad de conexión, especifique "property1=com.ibm.as400.access.AS400JDBCDriver;translate binary=true".
4. Cree un asesoramiento utilizando el Creador de asesoramientos. Abra el Creador de asesoramientos pulsando Reforzar > Asesoramiento de vulnerabilidades > Creador de asesoramientos.
    a. Especifique una descripción para el asesoramiento.
    b. Añada el origen de datos creado en el paso anterior pulsando Añadir origen de datos, y seleccione el origen de datos en el Buscador de orígenes de datos, y pulse Añadir.
    Nota: Debe pulsar Aplicar para guardar el asesoramiento antes de configurar las pruebas.
5. Añada pruebas al asesoramiento pulsando Configurar pruebas. Pulse el separador IBM para i, seleccione las pruebas que desea añadir y pulse Añadir selecciones.
6. Pulse Volver para volver al Buscador de asesoramiento de vulnerabilidades. Ejecute la prueba pulsando Ejecutar una vez ahora, o planifique la prueba utilizando el Creador de procesos de auditoría.. Abra el creador de procesos de auditoría pulsando Descubrir > Clasificaciones > Creador de procesos de auditoría.
7. Seleccione Ver resultados para visualizar los detalles de todas las pruebas ejecutadas, incluidas las recomendaciones para mejorar la puntuación.

Resultados

¿Qué hacer cuando falla una prueba?

- Revisar en la base de datos si está relacionada con parches.
- Volver a configurar los parámetros de base de datos en las prácticas recomendadas
- Revocar objetos o privilegios del sistema que no las aplicaciones no necesiten.
- Revocar los objetos concedidos directamente al receptor de autorización, otorgar privilegios de objeto a un rol/grupo y asignar al receptor de autorización a dicho rol/grupo
- Modificar la configuración de política de contraseñas o cambiar la contraseña de los usuarios predeterminada.
- Si la aplicación necesitaba una concesión específica, puede crear un grupo de excepciones, enlazarlo a la prueba con fallos y volver a ejecutarla.

Tema principal: Inicio al asesoramiento de vulnerabilidades de Guardium

Utilización del asesoramiento de vulnerabilidades con Cloudera

Aprenda a utilizar el asesoramiento de vulnerabilidades de Guardium con las distribuciones de Cloudera de Apache Hadoop.

Cloudera Manager

Configuración de origen de datos

El origen de datos de Cloudera Manager utiliza la API Java de Cloudera Manager para establecer conexión. No utiliza JDBC.

El nombre de clúster debe estar definido en la GUI del origen de datos. Es el nombre de visualización de clúster en la parte izquierda de la interfaz gráfica de usuario de Cloudera manager.

Para ejecutar pruebas de asesoramiento de vulnerabilidades para Cloudera Manager, debe definir un usuario de origen de datos con el rol de sólo lectura para la mayoría de las pruebas de asesoramiento de vulnerabilidades. A continuación, hay un número pequeño de pruebas de asesoramiento de vulnerabilidades que requieren que el usuario del origen de datos tenga el rol de administrador como privilegio mínimo para ejecutar las pruebas.

Las siguientes pruebas de asesoramiento de vulnerabilidades requieren que el usuario del origen de datos tenga el rol de administrador de clústeres:

1. Orden de fondo de autenticación
2. Puerto HTTP para consola de administración
3. Puerto HTTPS para consola de administración
4. Utilización de la autenticación de TLS de los agentes en el servidor
5. Utilización del cifrado de TLS para la consola administrativa
6. Utilización del cifrado de TLS para agentes

Esta información también está disponible en el script gdmmonitor de Cloudera Manager(/log/var-log-guard/gdmmonitor_scripts/gdmmonitor-Cloudera-Manager.sql).

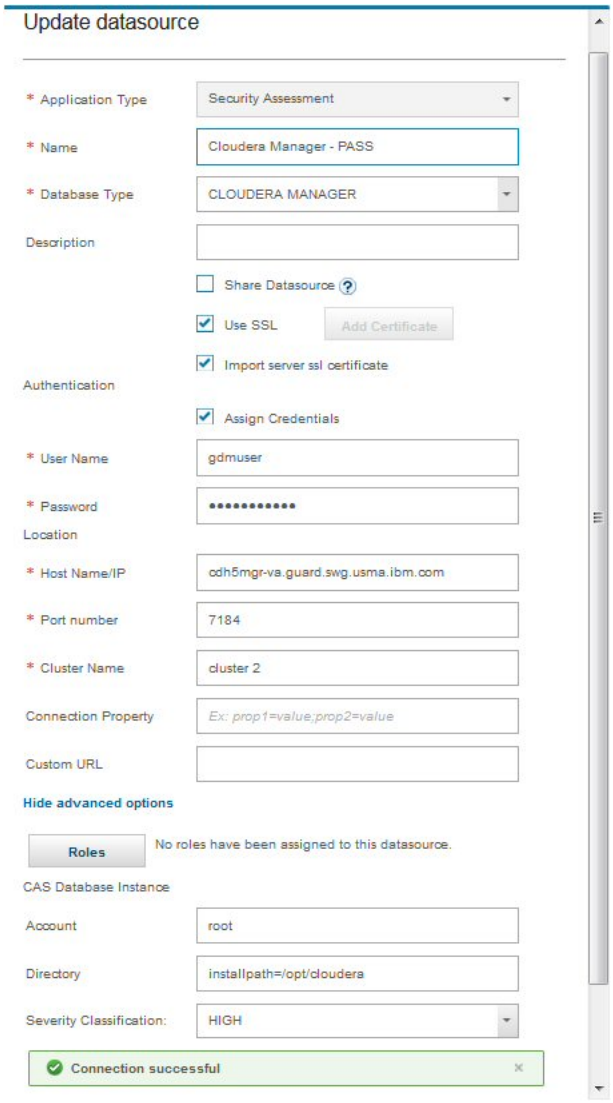
Si SSL está habilitado, compruebe "utilizar SSL" e "Importar certificado ssl de servidor"

Configuración de instancia de base de datos de CAS

La cuenta debe ser raíz.

El directorio se deberá definir como la vía de acceso de instalación de Cloudera Manager. Por ejemplo: installpath=/opt/cloudera

Ejemplo de valores de origen de datos de Cloudera Manager.



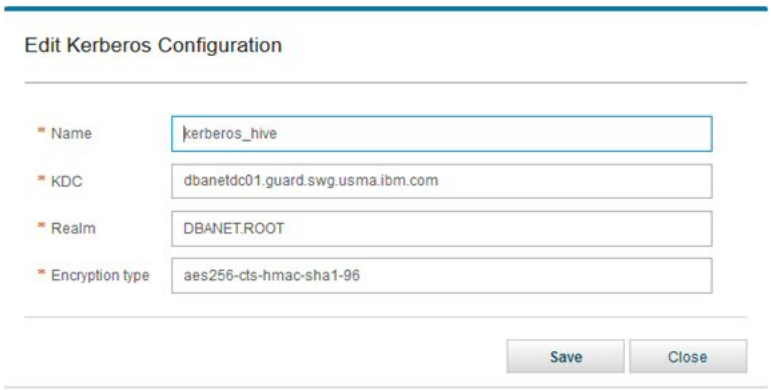
Hive

Configuración de origen de datos

Utilice el controlador JDBC 1.1.1 de Apache Hive.

Kerberos: El nombre de usuario y la contraseña deben ser un ID de usuario y una contraseña de Kerberos válidos. También se utiliza en CA. Se trata de una prueba para asegurarse de que el ID de usuario y la contraseña de Kerberos pueden utilizarse para iniciar sesión en la línea de mandatos beeline de Hive.

Asegúrese de que ya ha creado una configuración de Kerberos que defina el KDC y el reino del dispositivo. En la GUI de Guardium, diríjase a Configuración > Herramientas y vistas > Configuración de Kerberos. Si no se ha creado ninguna configuración de Kerberos, pulse en el icono + para crear una nueva configuración.



Después de haber creado una configuración de Kerberos, puede seleccionarla para realizar la configuración del origen de datos.

Si SSL está habilitado, marque el recuadro "Utilizar SSL" y, a continuación, "Importar certificado ssl de servidor".

Nota: Hive solo puede dar soporte a LDAP/SSL o Kerberos, pero no a ambos.

Configuración de una instancia de base de datos de CAS

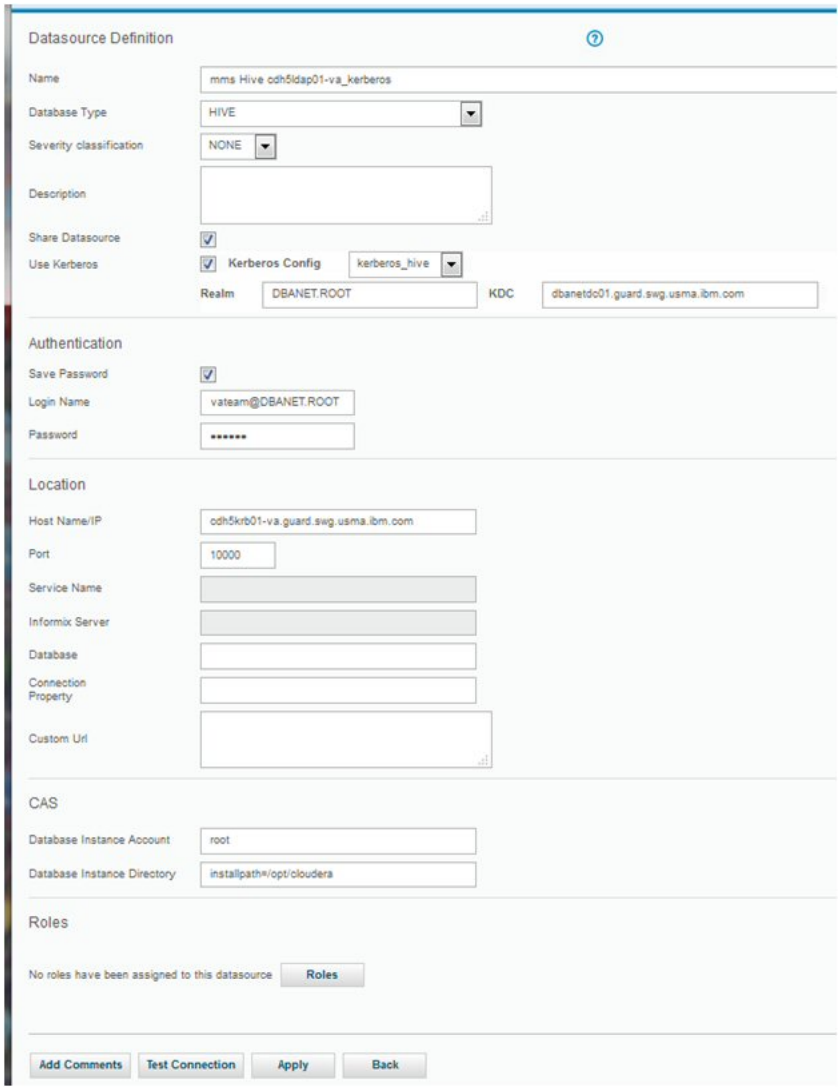
1. El directorio se deberá definir como la vía de acceso de instalación de Cloudera Manager. Por ejemplo: installpath=/opt/cloudera
2. Si se habilita HDFS para Kerberos, el nombre de usuario y contraseña del origen de datos deben ser un ID de usuario y una contraseña de Kerberos válidos. Los scripts de CAS lo utilizan para obtener un certificado de Kerberos.
3. La cuenta debe ser raíz. Para ciertas pruebas de parámetro que requieren CAS, es importante que el usuario de CAS sea raíz para poder acceder a la configuración en tiempo real desde el directorio de proceso del agente Cloudera (/var/run/cloudera-scm-agent/process/).

Nota: Guardium no modifica ni altera de ninguna manera los datos de configuración.

Para Hive

Para las pruebas de privilegio, la cuenta de origen de datos debe ser un miembro del grupo de administración de Sentry. Consulte el script gdmmonitor de Hive para obtener los pasos i verificar el grupo de administración de sentry.

Al configurar orígenes de datos de Hive, solo puede realizar una conexión de prueba JDBC cuando el origen de datos apunte a Hiveserver2. Para el resto de los orígenes de datos de Hive puede clonar dicho origen de datos utilizando el nodename en el que está instalado el servicio de Cloudera. Asegúrese de que el origen de datos clonado tiene un nombre de usuario y una contraseña válidos igual que el origen de datos de Hive server2. Para estos orígenes de datos, no puede realizar una conexión de prueba de origen de datos. Sin embargo, Guardium depende de la exactitud del nombre de usuario y contraseña del origen de datos para realizar una conexión de Kerberos utilizando CAS cuando Kerberos está habilitado.



Pruebas de asesoramiento de vulnerabilidades

Las pruebas Privilegio de Hive requieren que los servicios de sentry estén instalados y configurados. Sin Sentry, no hay seguridad. Todo el mundo puede conectarse a Hive y los datos de acceso.

La prueba de CAS de asesoramiento de vulnerabilidades para los parámetros HDFS se realiza a partir de los archivos de configuración del directorio de proceso de Cloudera Agent. Los nombres de carpeta de estos directorios de proceso cambian cada vez que se inician los servicios de Cloudera Agent.

Algunas de las pruebas de CAS de los parámetros HDFS requieren que la configuración de nodo del sistema de origen de datos sea específica (por ejemplo, NameNode o DataNode). Algunas pruebas de CAS requieren que se instalen Yarn, Mapreduce o Hive Server en el sistema de origen de datos. Seleccione las pruebas con cuidado para el asesoramiento basado en la configuración del sistema del origen de datos. Si no se cumplen los requisitos para la prueba, esta generará un error con una recomendación de ejecución de las pruebas en los servicios de Cloudera correctos. Los requisitos también se mencionan en la descripción de la prueba.

Si crea un origen de datos de Hive, se recomienda tener un origen de datos para cada servicio de Cloudera (NameNode, DataNode, HiveServer2, Hivemetastore, Yarn NodeManager y Yarn ResourceManager).

Independientemente del número de nodos del clúster, si tiene un origen de datos de Guardium Hive que cubra todos estos servicios, habrá configurado correctamente el entorno para ejecutar el asesoramiento de vulnerabilidades.

Por ejemplo

Tema principal: Inicio al asesoramiento de vulnerabilidades de Guardium

Pruebas de asesoramiento de vulnerabilidades

Guardium proporciona varios tipos de pruebas que le permiten evaluar la vulnerabilidad.

Pruebas de asesoramiento de vulnerabilidades

Guardium proporciona más de doscientas pruebas predefinidas para comprobar parámetros de configuración de base de datos, privilegios y otras vulnerabilidades. También puede definir sus propias pruebas.

Un asesoramiento de vulnerabilidades puede contener uno o varios de los siguientes tipos de pruebas.

Pruebas predefinidas

Las pruebas predefinidas están diseñadas para ilustrar problemas comunes de vulnerabilidad que se pueden encontrar en entornos de base de datos. A causa de la naturaleza altamente variable de las aplicaciones de base de datos y las diferencias en lo que se considera aceptable en varias empresas o situaciones, algunas de estas pruebas pueden ser adecuadas para determinadas bases de datos, pero completamente inapropiadas para otras (incluso dentro de la misma empresa). La mayoría de las pruebas predefinidas son personalizables para satisfacer los requisitos de su organización. De forma adicional, para mantener los asesoramientos al corriente con las mejores prácticas del sector y protegerlos frente a las vulnerabilidades recién descubiertas, Guardium distribuye nuevas pruebas de asesoramiento y las actualiza trimestralmente como parte de su servicio de suscripción de protección de base de datos. Consulte la guía de administración de Guardium para obtener más detalles.

Las pruebas predefinidas incluyen:

- Pruebas de comportamiento
- Pruebas de configuración

Pruebas de comportamiento

Este conjunto de pruebas asesora el estado de seguridad del entorno de base de datos mediante la observación del tráfico de base de datos en tiempo real y el descubrimiento de vulnerabilidades en la forma en la que se está accediendo y manipulando la información.

A modo de ejemplo, algunas de las pruebas de vulnerabilidad de comportamiento son:

- Acceso de usuarios predeterminados
- Infracciones de las reglas de acceso
- Ejecución de los mandatos de administración, DDL y DBCC directamente desde los clientes de base de datos
- Errores de inicio de sesión excesivos
- Errores SQL excesivos
- Inicios de sesión después de horas laborables
- Inicios de sesión de administrador excesivos
- Comprobaciones de las llamadas a los procedimientos almacenados ampliados
- Comprobaciones de que no se haya accedido a los ID de usuario desde varias direcciones de IP

Pruebas de configuración

Este conjunto de asesoramientos comprueba los valores de configuración relacionados con la seguridad de las bases de datos de destino, buscando errores comunes o fallos en la configuración de vulnerabilidades.

A modo de ejemplo, las categorías actuales con algunas pruebas de alto nivel son las siguientes:

- Privilegio
  - Creación de objetos / derechos de uso
  - Concesión de privilegios a DBA y usuarios individuales
  - Derechos de nivel de sistema
- Autenticación
  - Uso de cuenta de usuario
  - Uso del inicio de sesión remoto
  - Normativa de contraseñas

- Configuración
  - Valores de parámetros específicos de base de datos
  - Valores de parámetros de nivel de sistema
- Versión
  - Versiones de base de datos
  - Niveles de parche de base de datos
- Objeto
  - Bases de datos de ejemplos instaladas
  - Diseños de base de datos recomendados
  - Propiedad de base de datos

Pruebas basadas en consultas

Una prueba basada en consultas es una prueba predefinida o definida por el usuario que se puede crear rápida y fácilmente al definir o modificar consultas SQL, que se ejecutarán en el origen de datos de la base de datos y en resultados en comparación con un valor de prueba predefinido. Consulte Definir una prueba basada en consultas para obtener información adicional sobre la creación de una prueba basada en consultas.

Pruebas basadas en CAS

Una prueba basada en CAS es una prueba predefinida o definida por el usuario basada en un elemento de plantilla de CAS de tipo del mandato de script de SO y que utiliza los datos recopilados de CAS.

Los usuarios pueden especificar el elemento de plantilla y probarlo con el contenido de los resultados de CAS. Consulte Crear un elemento de conjunto de plantillas nuevo para obtener ayuda sobre la creación de una plantilla de CAS de tipo de script de OS.

Guardium también viene preconfigurado con algunos elementos de plantilla de CAS de tipo de script de SO que se pueden utilizar para crear una prueba basada en CAS. Estas pruebas se pueden ver mediante el panel Definición de conjunto de plantillas de CAS y tienen un nombre que contiene la palabra *Asesoramiento*. Por ejemplo, el conjunto Unix/Oracle para asesoramientos se denomina Asesoramiento de Unix/Oracle de Guardium. Además, cualquier plantilla que se añada que implique permisos de archivo también se utilizará para la comprobación de permisos y propiedad. Consulte Modificar un elemento de conjunto de plantillas para ver estos conjuntos de plantillas y los elementos con el tipo de script de SO.

Tanto si utiliza Guardium preconfigurado o define uno propio, una vez definido, estas pruebas aparecerán para que las pueda seleccionar durante la creación o modificación de pruebas basadas en CAS. Consulte Definir una prueba basada en CAS para obtener información adicional.

Pruebas de CVE

Guardium supervisa constantemente las vulnerabilidades y exposiciones comunes (CVE) de MITRE Coporation y añade estas pruebas para las vulnerabilidades relacionadas con la base de datos relevante.

- Definición de una prueba basada en consultas
  Cree una prueba basada en una consulta que ejecuta una sentencia SQL.
- Definición de pruebas basadas en CAS
  Los asesoramientos de vulnerabilidades utilizan el mecanismo de CAS para ejecutar pruebas a nivel de SO en el servidor de base de datos e identificar vulnerabilidades.

Tema principal: Asesorar y reforzar

Definición de una prueba basada en consultas

Cree una prueba basada en una consulta que ejecuta una sentencia SQL.

Acerca de esta tarea

Puede crear una nueva prueba basada en consulta utilizando cualquiera de los métodos siguientes:

Nueva
: Empezar desde el principio y definir todos los campos.

Clonación
: Clonar una prueba basada en consulta existente.

Modificación
: Modificar una prueba basada en consultas existente.

Procedimiento

1. Abra el Creador de asesoramientos pulsando Reforzar > Asesoramiento de vulnerabilidades > Creador de asesoramientos.
2. En las pruebas definidas por el usuario, pulse Pruebas basadas en consultas.
3. Pulse Nueva, Clonar o Modificar para abrir el Creador de pruebas basadas en consultas.
4. Especifique un Nombre de prueba exclusivo.
5. Seleccione un Tipo de base de datos.
6. Seleccione una Categoría.
7. Seleccione una Gravedad.
8. Opcional: Especifique una Descripción breve para la prueba.
9. Opcional: Especifique una Referencia externa para la prueba.
10. Especifique el Texto de resultado para pasar que se visualizará cuando se pase la prueba.
11. Especifique el Texto de resultado cuando falle que se mostrará cuando falle la prueba.
12. Especifique la Sentencia SQL que se ejecutará en la prueba.

    Utilice la convención siguiente para añadir y hacer referencia a miembros de grupos en la sentencia SQL:

    Por ejemplo:

Para hacer referencia a un grupo de usuarios definido para el grupo MyUsersGroup y sustituirlo por los miembros reales del grupo utilice:

```
Select ... from DBA_GRANTS where ... AND USER in (~~G~MyUsersGroup~~) and ...
```

Como resultado se obtendrá una sentencia SQL como la siguiente, en la que U1, U2, etc., son los miembros del grupo MyUserGroup:

```
Select ... from DBA_GRANTS where ... AND USER in ('U1','U2','U3',...) and ...
```

Si el grupo no tiene miembros, la base de datos devuelve un error. En este caso, la referencia se sustituye por un único par de comillas, de la forma siguiente:

```
Select ... from DBA_GRANTS where ... AND USER in ('') and ...
```

Utilice la convención siguiente para reemplazar una referencia a un alias específico (de un tipo de grupo específico) por el alias real:

Por ejemplo:

Select ... from USER_OBJECTS where ... AND OBJECT_TYPE = '~~A~GroupType~TYPE~~'

Si hay un alias en TYPE del tipo de grupo GroupType, reemplazará la serie y el SQL resultante será el siguiente:

Select ... from USER_OBJECTS where ... AND OBJECT_TYPE = 'TYPE'

donde TYPE es el ALIAS real

13. Opcional: Especifique una Sentencia SQL para detalles, una sentencia SQL que recupera una lista de series para generar una serie de detalles de Detalle de prefijo + lista de series. Consulte el ejemplo en Detalle de prefijo.
    Nota: El detalle generado solo se visualiza cuando la prueba basada en consultas falla; lo que permite al usuario especificar una sentencia SQL que puede recuperar la información que ha hecho que la prueba falle y ayudar a identificar la causa del fallo.
    Nota: La serie de detalle se puede ver en Resultados de asesoramientos de seguridad, pulsando en el nombre de prueba de asesoramiento y también a través del atributo Detalles de resultados de la entidad Resultado de la prueba.
14. Opcional: Especifique una sentencia SQL de comprobación previa a la prueba. Esta sentencia se ejecuta antes de la ejecución de la prueba. Si la sentencia devuelve 0, la prueba no se ejecuta. Si la prueba devuelve 1 o error, la prueba se ejecuta.
15. Opcional: Especifique un Mensaje de fallo previo a la prueba. Este mensaje se introduce en los resultados del asesoramiento si la prueba no se ejecuta porque la sentencia SQL devuelve 0.
16. Opcional: En Bases de datos de bucle, especifique una lista de bases de datos mediante la cual debe realizarse un bucle en la prueba. La prueba devuelve la unión o la suma de los resultados devueltos de todas las bases de datos especificadas. Puede utilizar esta función solo cuando la prueba devuelva un valor entero, y solo con estos tipos de base de datos: Informix, SQL Server, Sybase SE, PostgreSQL y MySQL. El bucle se ejecuta si se ha marcado el recuadro Distintivo de bucle de BD. Es posible que una o varias de las bases de datos especificadas no estén disponibles cuando se ejecute la prueba. En ese caso, la prueba omitirá la base de datos y continuará, o se detendrá y emitirá un mensaje de fallo, en función de si se ha seleccionado el recuadro Omitir con error.
17. Opcional: Especifique un Detalle de prefijo que aparecerá al principio de la serie de detalle.

```
Example for SQL Statement for Detail & Detail prefix:
Test that checks for objects with certain grants.
Detail prefix: "Objects found with certain GRANT:"
SQL Statement for Detail: SELECT object FROM....--returning 4 records:
      Obj1
      Obj2
      Obj3
      Obj4
==> Details: Objects found with certain GRANT: Obj1, Obj2, Obj3, Obj4
```

18. Opcional: Marque el recuadro de selección Vincular variable de salida si el texto especificado en la sentencia SQL es un bloqueo de procedimientos del código que devolverá un valor que debería estar enlazado a una variable de Guardium interna que se utilizará en la comparación en el valor Comparar con.

```
Example (Oracle):
declare
    retval integer := 0;
    strval varchar2(255) := '';
    nver number;
    sver varchar2(255) := '';
begin
    select VERSION
    into sver
    from V$INSTANCE;
    nver := to_number(substr(sver,1,(instr(sver,'.',1,2) - 1)));
    if nver >= 11.1 then
        select VALUE
        into strval
        from V$PARAMETER
        where NAME = 'sec_case_sensitive_logon';
    end if;
    if (nver < 11.1 or strval = 'TRUE') then
        retval := 0;
    else
        retval := 1;
    end if;
    ? := retval;
end;
```

19. Seleccione el Tipo de retorno que se devolverá de la sentencia SQL.
20. Seleccione el operador que se utilizará para la condición.
21. Entre en Comparar con valor, que se utilizará para comparar con el valor de retorno de la sentencia SQL utilizando el operador de comparación. Esta comparación es la que determina si se ha pasado la prueba o si ha fallado. También puede pulsar RE (expresión regular) para definir una expresión regular para el valor de comparación.
22. Realice una de las siguientes acciones:
    - Pulse Atrás para cancelar los cambios y vuelva a la pantalla anterior.
    - Pulse Aplicar para guardar la prueba basada en consulta.

Resultados

Puede añadir esta prueba basada en consultas recién creada a un asesoramiento.

Qué hacer a continuación

Tema principal: Pruebas de asesoramiento de vulnerabilidades

Definición de pruebas basadas en CAS

Los asesoramientos de vulnerabilidades utilizan el mecanismo de CAS para ejecutar pruebas a nivel de SO en el servidor de base de datos e identificar vulnerabilidades.

Antes de empezar

Acerca de esta tarea

Puede crear una prueba basada en CAS nueva modificando una existente, o puede empezar desde el principio y definir todos los campos.

Procedimiento

1. Abra Creador de asesoramientos pulsando Reforzar > Asesoramiento de vulnerabilidades > Creador de asesoramientos.
2. En las pruebas definidas por el usuario, pulse Pruebas basadas en CAS para abrir el panel Buscador de pruebas basadas en CAS.
3. Pulse Nueva o Modificar para crear una prueba nueva.
4. Especifique un Nombre de prueba exclusivo.
5. Seleccione una base de datos del menú Tipo de base de datos.
6. Seleccione una categoría del menú Categoría.
7. Seleccione una categoría del menú Gravedad.
8. Opcional: Especifique una Descripción breve para la prueba.
9. Opcional: Especifique una Referencia externa para la prueba.
10. Especifique un Texto de resultado para pasar, que se mostrará cuando se pase la prueba.
11. Especifique un Texto de resultado para fallar, que se mostrará cuando la prueba falle.
12. Especifique un Texto de recomendación para pasar, que se mostrará cuando se pase la prueba.
13. Especifique Texto de recomendación para fallar, que se mostrará cuando la prueba falle. Texto de recomendación para fallar: para evitar un ataque informático entre sitios, se volverá a escribir cualquier nombre de esta lista utilizado en el recuadro Texto de recomendación para fallar: expression; function; javascript; script; alert; eval; ContentType
14. Seleccione una plantilla para utilizarla en el menú Plantilla de CAS.
15. Seleccione un operador para utilizarlo en el menú operador.
16. Especifique una Serie de búsqueda que se utilizará con el operador para comparar lo que se devuelve de la plantilla de CAS. Esta comparación es la que determina si se ha pasado la prueba o si ha fallado. También puede pulsar en el icono RE para definir una expresión regular de la serie de búsqueda.
17. Opcional: Marque el recuadro de selección Fallo si coincide si la prueba debe fallar cuando se produce una coincidencia con la serie de búsqueda.
18. Pulse Aplicar para guardar la prueba basada en CAS.

Resultados

Puede añadir esta nueva prueba basada en CAS a un asesoramiento.
Tema principal: Pruebas de asesoramiento de vulnerabilidades

Asesoramientos

Los asesoramientos son un grupo de pruebas que escanean las infraestructuras de base de datos en busca de vulnerabilidades y proporcionan una evaluación de la salud de seguridad de la base de datos y de los datos con medidas históricas y en tiempo real.

- Creación de un asesoramiento
  Cree un asesoramiento, o modifique o clone uno existente.
- Creación de una excepción de prueba de VA
  Utilice una excepción de prueba para excluir los miembros específicos de un grupo de un asesoramiento de seguridad. Ejecute el asesoramiento de seguridad en el grupo de excepciones para ver si un miembro específico de un grupo está afectando a los resultados de la evaluación. Esto es útil si no desea o no está autorizado a cambiar los valores del grupo.
- Cómo crear un asesoramiento de seguridad
  Ejecute asesoramientos de seguridad en los orígenes de datos seleccionados para identificar y direccionar de forma proactiva las vulnerabilidades, mejorar las configuraciones y fortalecer las infraestructuras.
- Ejecución de un asesoramiento
  Para obtener los resultados de un asesoramiento, este se debe ejecutar una vez se haya creado.
- Visualización de resultados de asesoramiento
  Puede realizar varias acciones mientras visualiza los resultados de un asesoramiento.
- Resumen del asesoramiento de vulnerabilidades
  La siguiente tabla lista información por prueba y clave de base de datos visualizada en la tabla de resumen asesoramiento de vulnerabilidades: resultado de la prueba por identificador único; antigüedad fallida acumulativa; primera fecha fallida / última fecha fallida; última fecha pasada; y última fecha escaneada. Se realiza un seguimiento de esta información y los usuarios pueden crear un informe sobre la misma.

Tema principal: Asesorar y reforzar

Creación de un asesoramiento

Cree un asesoramiento, o modifique o clone uno existente.

Antes de empezar

Abra el Creador de asesoramientos pulsando Reforzar > Asesoramiento de vulnerabilidades > Creador de asesoramientos.

Acerca de esta tarea

Procedimiento

1. En el panel Buscador de asesoramientos de seguridad, pulse Nuevo para crear un asesoramiento completamente nuevo. Pulse Clonar o Modificar para trabajar con un asesoramiento existente. Al pulsar cualquiera de estos botones se abre el panel Creador de asesoramientos de seguridad. Si está creando un asesoramiento completamente nuevo, realice los pasos siguientes. Si está clonando o modificando un asesoramiento existente, especifique una nueva descripción y, a continuación, modifique solo los campos que desea cambiar.
2. Especifique una Descripción exclusiva para el asesoramiento
3. Añada un origen de datos pulsando Añadir origen de datos, introduzca la información necesaria y seleccione Añadir.
4. Añada pruebas al asesoramiento pulsando Configurar pruebas.
    a. En el panel Pruebas disponibles para ser añadidas, seleccione el separador adecuado para el origen de datos que ha añadido anteriormente.
    b. Seleccione las pruebas que desee y pulse Añadir selecciones para agregarlas al asesoramiento. Una vez añadidas, las selecciones aparecerán en el panel Selecciones de pruebas de asesoramiento.
    c. Utilice Selecciones de pruebas de asesoramiento para gestionar las pruebas de su asesoramiento. Suprima cualquier prueba seleccionada, o pulse Ajustar el ajuste de esta prueba para personalizar los parámetros de la prueba.
5. Añadir roles al asesoramiento.
   Nota: No puede asignar roles a un asesoramiento hasta que haya asignado roles a los orígenes de datos en los que se basa.
6. Pulse Aplicar para guardar el asesoramiento.

   Pulse Soporte de CAS para proporcionar los datos adecuados para el asesoramiento.

   También puede Añadir comentarios a cualquier asesoramiento para documentar o registrar los cambios que se han realizado en el asesoramiento y la razón por la que se han realizado.

Resultados

El nuevo asesoramiento está listo para ejecutarse.
Tema principal: Asesoramientos

Creación de una excepción de prueba de VA

Utilice una excepción de prueba para excluir los miembros específicos de un grupo de un asesoramiento de seguridad. Ejecute el asesoramiento de seguridad en el grupo de excepciones para ver si un miembro específico de un grupo está afectando a los resultados de la evaluación. Esto es útil si no desea o no está autorizado a cambiar los valores del grupo.

Procedimiento

1. Abra el Creador de grupos pulsando Configuración > Herramientas y vistas > Creador de grupos.
2. Seleccione Excepción de pruebas de asesoramiento de vulnerabilidades del menú Tipo de grupo para visualizar la lista de grupos de excepción predefinidos.
3. Seleccione un grupo del menú Modificar grupos existentes y pulse Modificar.
4. Añada los miembros del grupo que desea excluir de la prueba de asesoramiento de vulnerabilidades.
5. Abra el Creador de asesoramientos pulsando Reforzar > Asesoramiento de vulnerabilidades > Creador de asesoramientos. Seleccione un asesoramiento de Buscador de asesoramiento de seguridad y pulse Configurar pruebas.
6. Encuentre la prueba en la que desea añadir la excepción y pulse el botón Ajustar este ajuste de prueba de la prueba en la columna Ajuste.
7. Seleccione el grupo de excepciones del menú y pulse Guardar. Ejecute el asesoramiento de nuevo para ver si el grupo de excepción afecta al resultado de la prueba.
   Nota: De forma predeterminada, Guardium incluye un grupo de excepciones denominado Exclusiones de usuario del perfil de IBM iSeries. Puede clonar y modificar este grupo para que se ajuste a sus necesidades.

   Todas las pruebas de privilegio de objetos de base de datos excluyen esquemas del sistema predeterminados de los grupos Guardium.

Tema principal: Asesoramientos

Cómo crear un asesoramiento de seguridad

Ejecute asesoramientos de seguridad en los orígenes de datos seleccionados para identificar y direccionar de forma proactiva las vulnerabilidades, mejorar las configuraciones y fortalecer las infraestructuras.

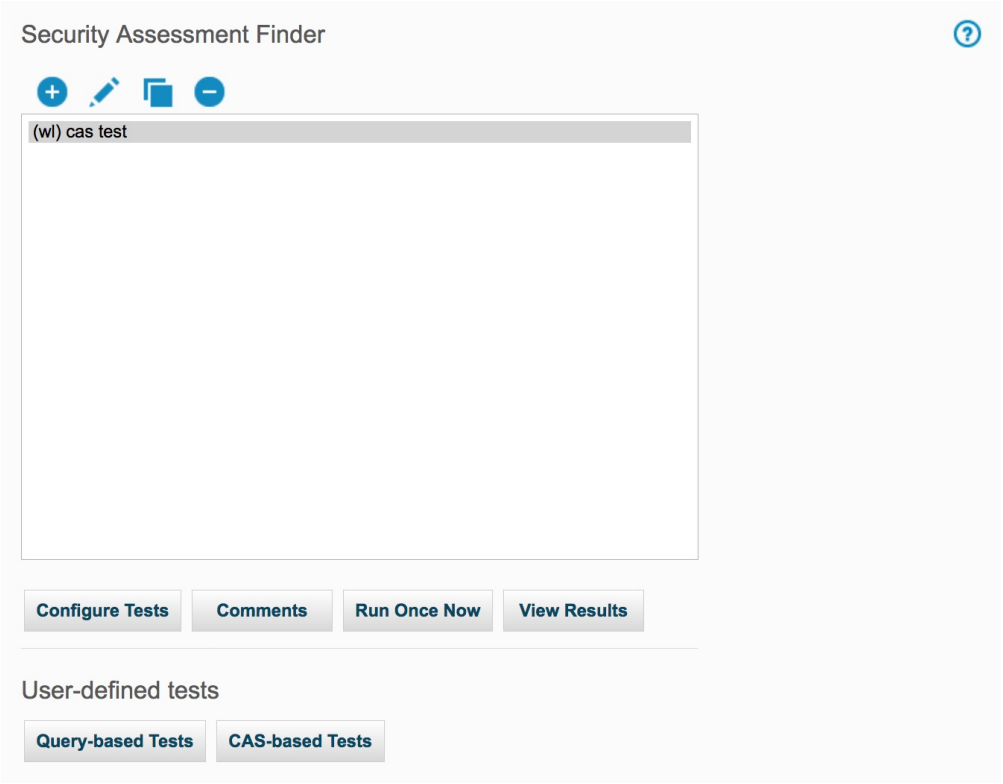
Acerca de esta tarea

Los pasos básicos para crear un asesoramiento de seguridad son:

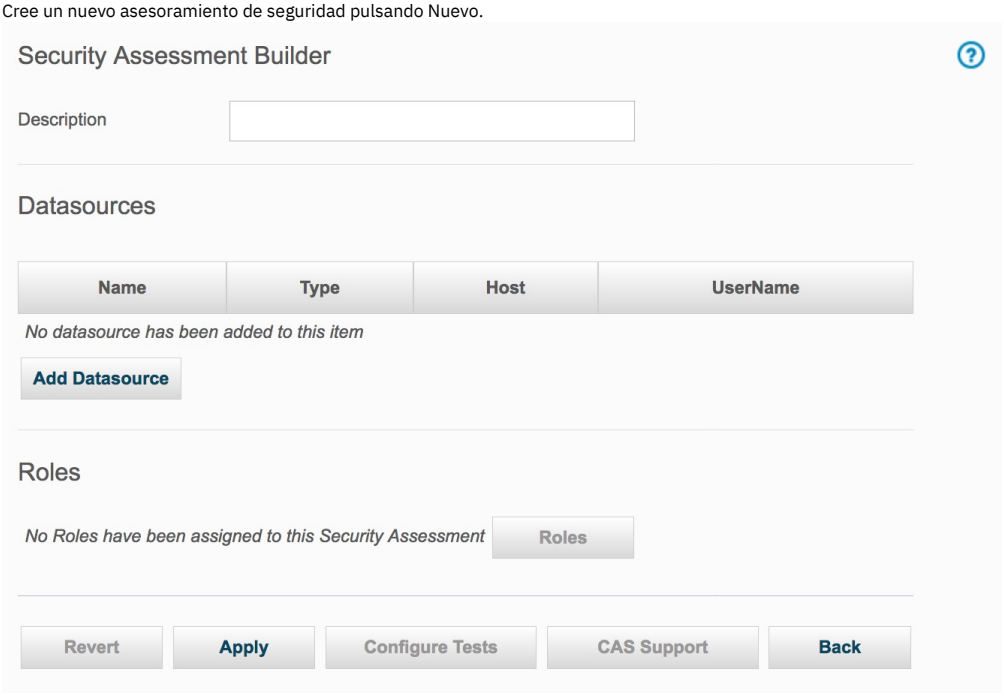
1. Crear el asesoramiento
2. Añadir orígenes de datos al asesoramiento
3. Añadir pruebas al asesoramiento

Procedimiento

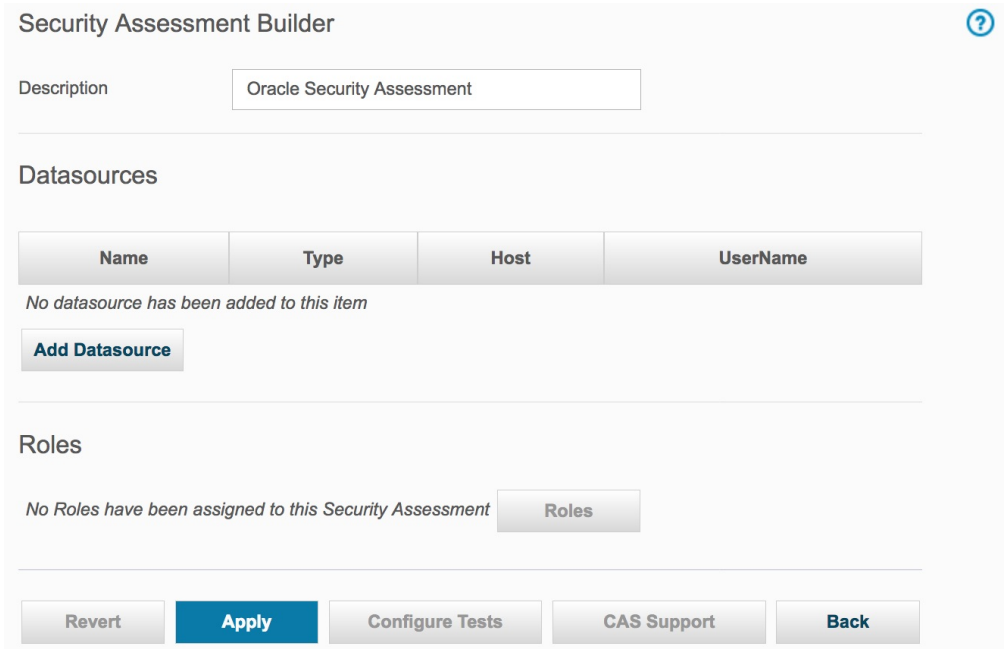
1. Cree o modifique un asesoramiento abriendo el Creador de asesoramientos. Abra el Creador de asesoramientos pulsando Reforzar > Asesoramiento de vulnerabilidades > Creador de asesoramientos.



2. Cree un nuevo asesoramiento de seguridad pulsando Nuevo.

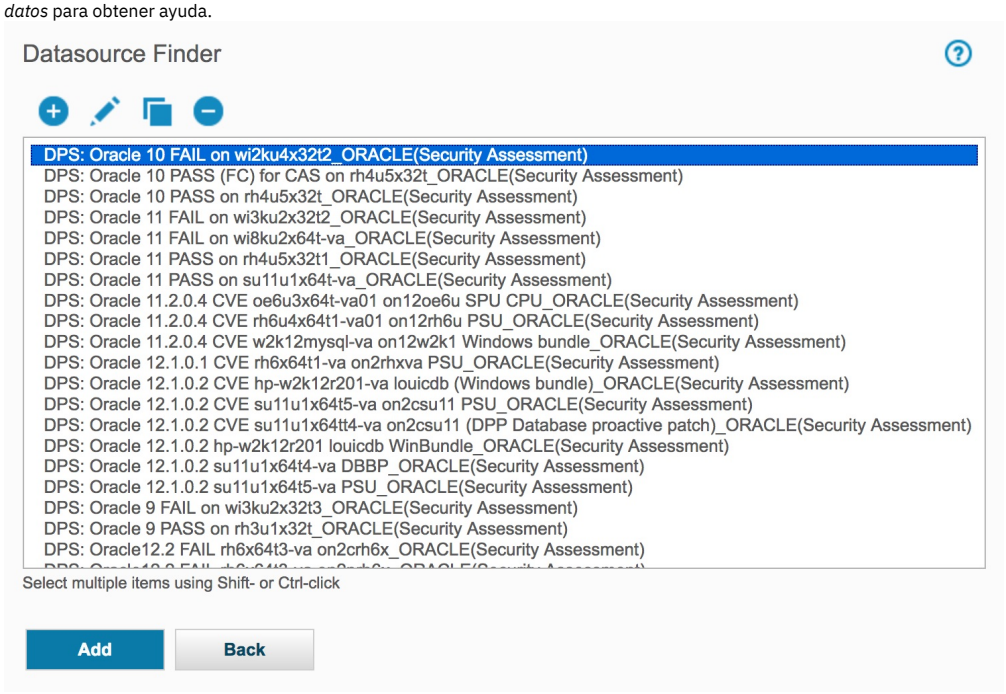


3. Especifique un nombre exclusivo para el asesoramiento en Descripción y pulse Aplicar para guardar la evaluación.

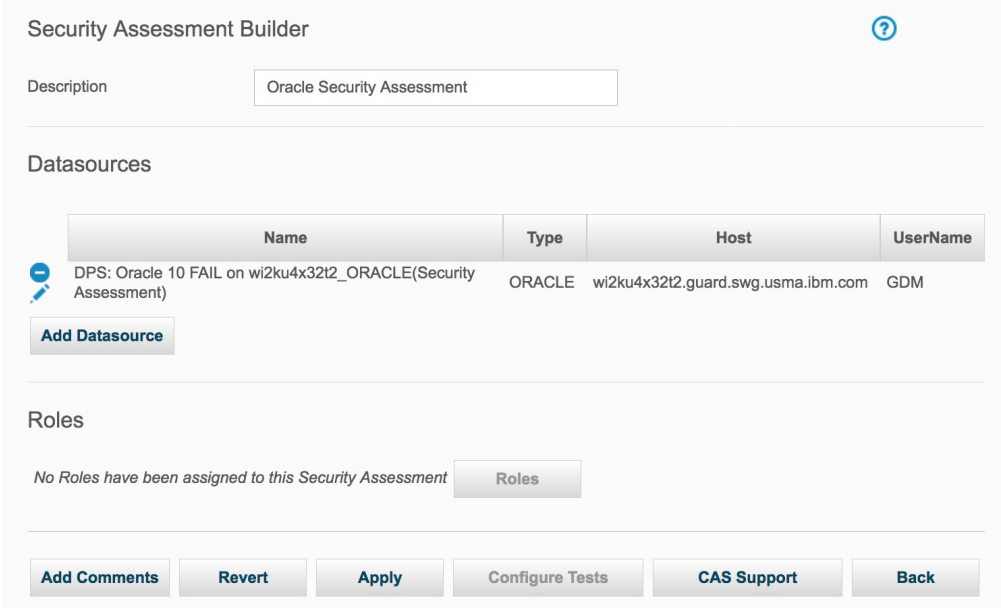


4. Añada un origen de datos al asesoramiento pulsando Añadir origen de datos. Seleccione un origen de datos de Buscador de orígenes de datos y pulse Añadir.

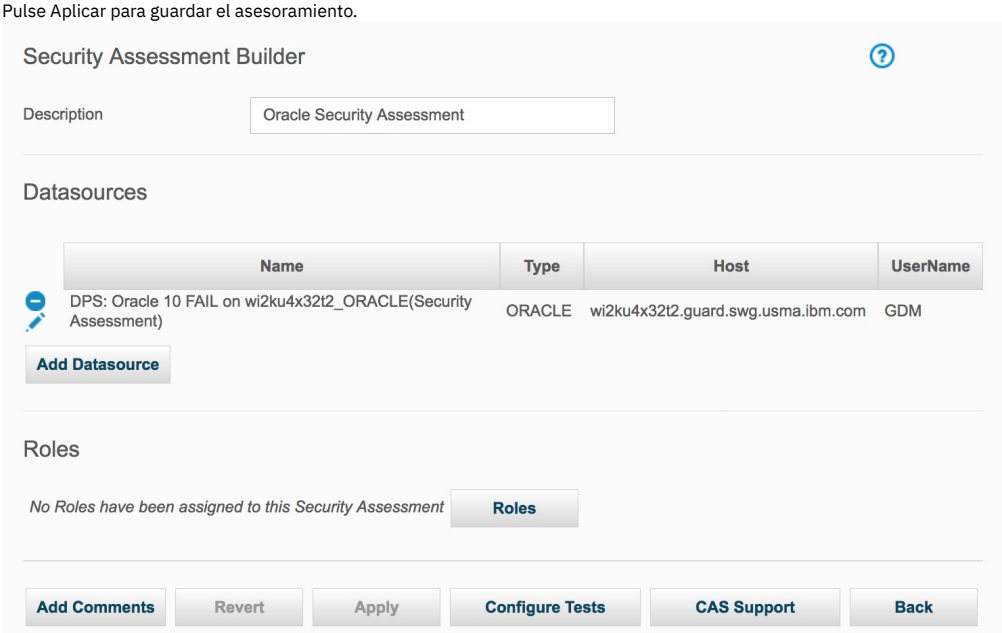
   Añada un origen de datos nuevo pulsando , completando la información de la ventana Definición de base de datos y pulsando Aplicar. Consulte *Orígenes de datos* para obtener ayuda.



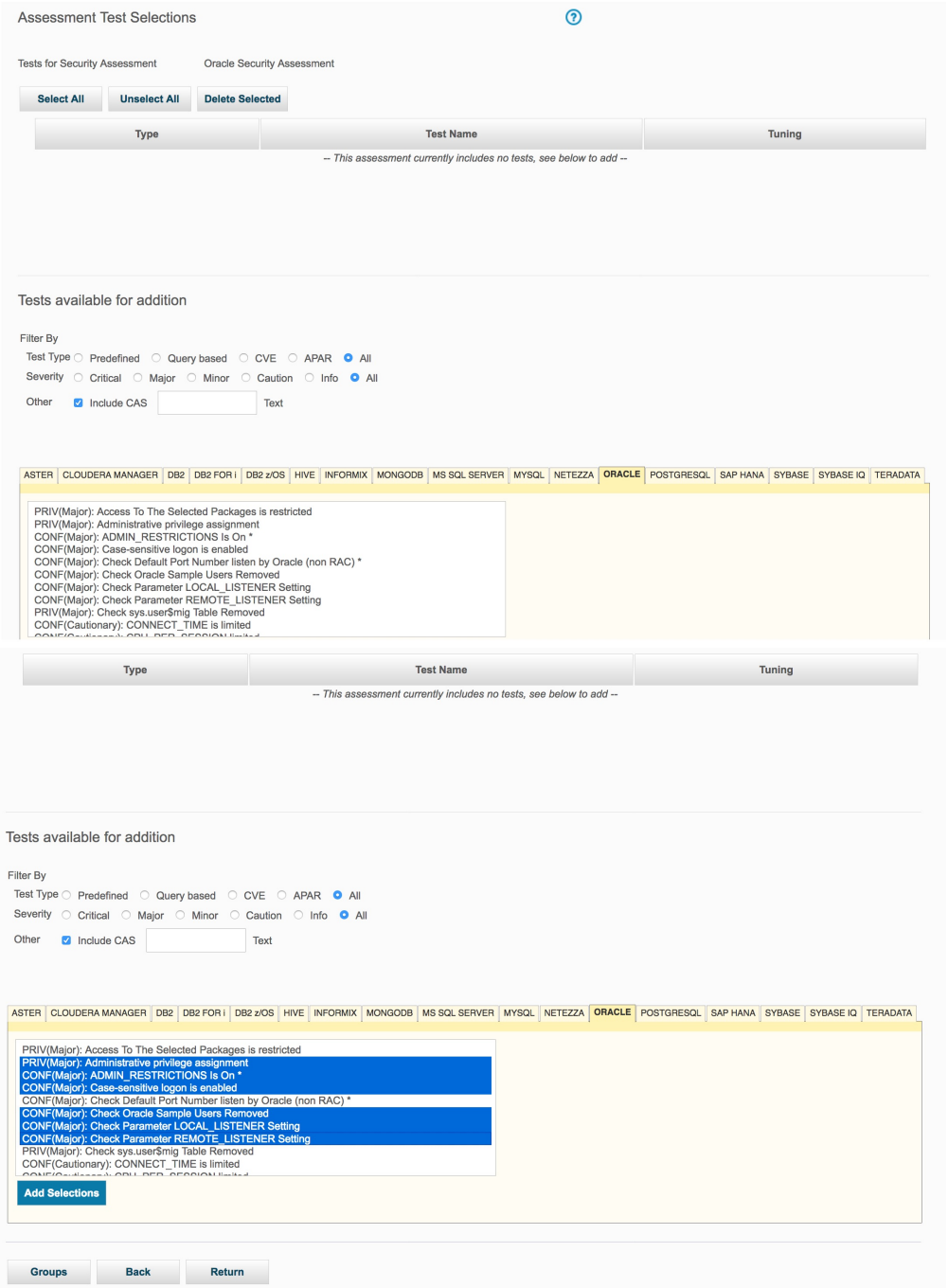
Después de pulsar el botón Añadir, el origen de datos aparecerá en la sección Orígenes de datos del Creador de asesoramientos de seguridad.

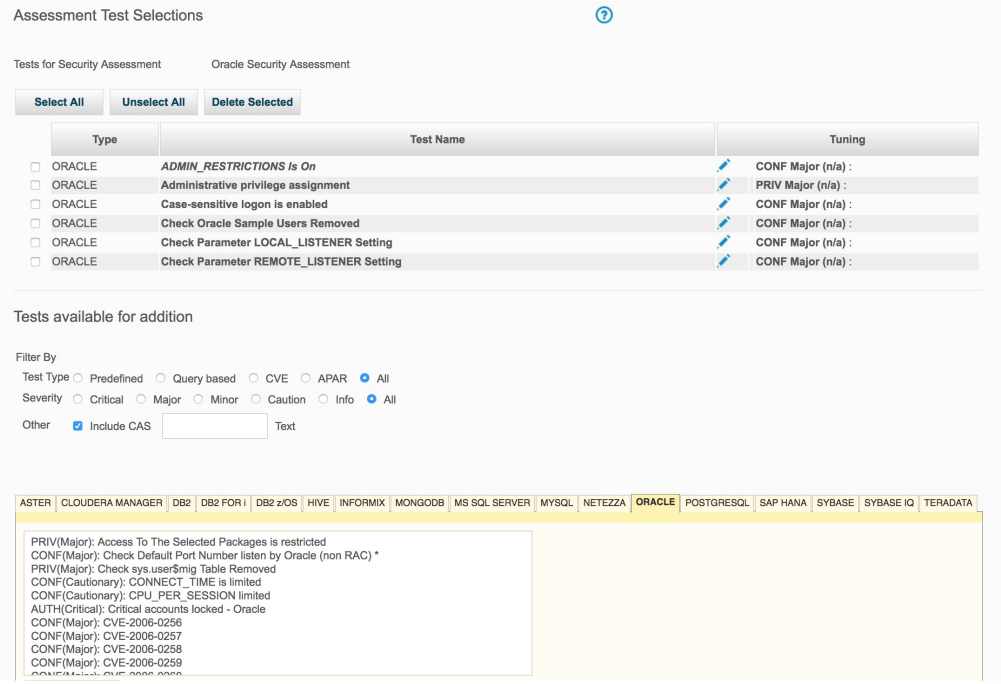


5. Pulse Aplicar para guardar el asesoramiento.



6. Pulse Configurar pruebas para añadir pruebas al asesoramiento. En el panel Pruebas disponibles para ser añadidas, pulse el separador del origen de datos adecuado que ha creado, seleccione las pruebas que desea añadir al asesoramiento y pulse Añadir selecciones. Utilice los botones de selección para filtrar las pruebas que se van a añadir. Consulte Pruebas predefinidas, Pruebas basadas en consulta, Pruebas de CVE o pruebas APAR para obtener ayuda.


Assessment Test Selections
Tests for Security Assessment
Oracle Security Assessment
Select All
Unselect All
Delete Selected
Type
Test Name
Tuning
-- This assessment currently includes no tests, see below to add --
Tests available for addition
Filter By
Test Type Predefined Query based CVE APAR All
Severity Critical Major Minor Caution Info All
Other Include CAS Text
ASTER CLOUDERA MANAGER DB2 DB2 FOR i DB2 z/OS HIVE INFORMIX MONGODB MS SQL SERVER MYSQL NETEZZA ORACLE POSTGRESQL SAP HANA SYBASE SYBASE IQ TERADATA
PRIV(Major): Access To The Selected Packages is restricted
PRIV(Major): Administrative privilege assignment
CONF(Major): ADMIN_RESTRICTIONS Is On *
CONF(Major): Case-sensitive logon is enabled
CONF(Major): Check Default Port Number listen by Oracle (non RAC) *
CONF(Major): Check Oracle Sample Users Removed
CONF(Major): Check Parameter LOCAL_LISTENER Setting
CONF(Major): Check Parameter REMOTE_LISTENER Setting
PRIV(Major): Check sys.user$mig Table Removed
CONF(Cautionary): CONNECT_TIME is limited
Type
Test Name
Tuning
-- This assessment currently includes no tests, see below to add --
Tests available for addition
Filter By
Test Type Predefined Query based CVE APAR All
Severity Critical Major Minor Caution Info All
Other Include CAS Text
ASTER CLOUDERA MANAGER DB2 DB2 FOR i DB2 z/OS HIVE INFORMIX MONGODB MS SQL SERVER MYSQL NETEZZA ORACLE POSTGRESQL SAP HANA SYBASE SYBASE IQ TERADATA
PRIV(Major): Access To The Selected Packages is restricted
PRIV(Major): Administrative privilege assignment
CONF(Major): ADMIN_RESTRICTIONS Is On *
CONF(Major): Case-sensitive logon is enabled
CONF(Major): Check Default Port Number listen by Oracle (non RAC) *
CONF(Major): Check Oracle Sample Users Removed
CONF(Major): Check Parameter LOCAL_LISTENER Setting
CONF(Major): Check Parameter REMOTE_LISTENER Setting
PRIV(Major): Check sys.user$mig Table Removed
CONF(Cautionary): CONNECT_TIME is limited
Add Selections
Groups
Back
Return



7. Pulse Atrás para volver al Creador de asesoramientos de seguridad, y seleccione Roles para añadir roles al asesoramiento.
   Nota: No puede asignar roles al asesoramiento hasta que haya asignado roles al origen de datos en el que se basa dicho asesoramiento.
8. Guarde el asesoramiento pulsando Aplicar. El asesoramiento ahora se puede ejecutar en los orígenes de datos seleccionados.

Tema principal: Asesoramientos

Ejecución de un asesoramiento

Para obtener los resultados de un asesoramiento, este se debe ejecutar una vez se haya creado.

Los asesoramientos se ejecutan en modalidad serializada uno tras otro. Si se ha planificado ejecutar más de un asesoramiento, se tendrán que poner en cola. Esta cola se puede ver mediante el informe de cola de trabajos de Guardium.

Al pulsar el botón Ejecutar una vez ahora se entrará al asesoramiento a la cola y se ejecutará inmediatamente. Es necesario un breve periodo de tiempo para que el trabajo se ejecute y se pueda visualizar. Consulte Visualización de resultados de asesoramiento para obtener más información acerca de los resultados de un asesoramiento.

Si lo desea, puede definir y planificar un proceso automático para ejecutar una definición de asesoramiento. El panel Buscador de procesos de auditoría es el punto de partida para crear o modificar una planificación de proceso de auditoría. Cree una planificación para ejecutar automáticamente sus asesoramientos accediendo al panel Buscador de procesos de auditoría. Consulte Automatización del flujo de trabajo de cumplimiento para obtener ayuda en la definición de un proceso de auditoría

Tema principal: Asesoramientos

Visualización de resultados de asesoramiento

Puede realizar varias acciones mientras visualiza los resultados de un asesoramiento.

Visualización de resultados de un asesoramiento

Visualice los resultados de una asesoramiento en el Creador de informes. Abra el Creador de informes haciendo clic en Reforzar > Informes > Creador de informes, y utilice los filtros para buscar el informe que desea.

Interpretación de los resultados de un asesoramiento

Un asesoramiento evalúa varias pruebas en base a varios informes. Los resultados globales se muestran en una ventana de navegador aparte titulada Resultados de asesoramientos de seguridad y tiene las secciones siguientes:

Identidad de asesoramiento

Los resultados de asesoramiento identifican:

- El nombre del asesoramiento
- La fecha y hora en que se ejecutó el asesoramiento
- El periodo de tiempo del asesoramiento
- Las direcciones IP o subredes del servidor y del cliente

Selección de asesoramiento

Utilice el menú desplegable para seleccionar y mostrar resultados anteriores de un asesoramiento. De forma predeterminada, se muestra el resultado más reciente.

Historial de resultados del asesoramiento

El Historial de resultados de asesoramiento muestra el porcentaje de pruebas que pasan durante un periodo de tiempo. En la sección Resultados de pruebas de asesoramiento se proporcionan más recomendaciones para mejorar el porcentaje de pruebas de paso.

Visualizar registro

Al pulsar, se mostrará el Registro de ejecución en una nueva ventana que muestra la ejecución de la prueba de asesoramiento. La indicación de fecha y hora, junto con los sucesos y los mensajes pueden ayudar en la depuración de problemas que pueden haber causado que determinadas pruebas fallen.

Resumen de resultados

Un gráfico tabular resume todas las pruebas que se han ejecutado en este asesoramiento. El eje X representa la gravedad de la prueba (CRÍTICA, MAYOR, MENOR, PRECAUCIÓN o INFO). El eje Y representa el tipo de prueba (Privilegio, Autenticación, Configuración, Versión, Otros). En la cuadrícula se encuentra la representación del número de pruebas que se han aprobado, han fallado o que han dado error al intentar ejecutarlas. Estos números están directamente relacionados con el detalle en las pruebas de asesoramiento que se proporcionan en la sección Resultados de pruebas de asesoramiento.

Filtro actual aplicado

Si desea cambiar el filtrado de lo que se ha aplicado, utilice las dos opciones siguientes para filtrar los resultados tal y como desee:

Restablecer filtrado: Elimina todas las opciones de filtrado seleccionadas a través de las opciones Controles de Ordenar / Filtrar.

Controles de Ordenar / Filtrar: Utilice esta opción para abrir las opciones ordenar/filtrar para el informe. Las opciones le permiten filtrar por gravedad, clasificación de gravedad de orígenes de datos (clasificación de gravedad de DS), puntuación (pasado, fallo, error) y tipos de prueba (observado/tipo de base de datos). La opción de clasificación permite clasificar las combinaciones de gravedad, puntuación y origen de datos. Pulse Aplicar cuando desee que se apliquen las opciones de filtro/clasificación elegidas.

Resultados de pruebas de asesoramiento

La sección Resultados de pruebas de asesoramiento proporciona una descripción detallada de las pruebas realizadas, información acerca del origen de datos de destino, la clasificación de la gravedad del origen de datos, y del estado de la prueba pasada/fallo, la gravedad, la referencia externa y la razón por la que se encuentra en el estado actual. Se pueden pulsar los nombres de prueba para filtrar toda la información fuera del informe, excepto la información relevante sobre dicha prueba en particular. En el campo Razón, una característica de ayuda contextual mostrará la recomendación para ayudar a remediar errores o pruebas con errores.

Los resultados del asesoramiento incluyen un recuento del número de pruebas y del número de pruebas pasadas en cada una de estas categorías:

- pruebas de CIS
- pruebas de CVE
- pruebas de STIG

Estos valores se muestran en el visor de resultados de asesoramiento y están disponibles para la creación de informes como parte del dominio de resultados del asesoramiento de vulnerabilidades.

Detalles del origen de datos

Cuando se expande, la sección Detalles de origen de datos mostrará todos los orígenes de datos a los que se ha hecho referencia en este asesoramiento, incluida la información de entorno específica del origen de datos.

información CVE y CVSS

Se mostrarán los registros de CVE y la información de CVSS en el visor de resultados de la prueba de asesoramiento.

Se pueden pulsar los enlaces de referencia (se abre una ventana nueva). Cada sección estará ausente cuando no haya ningún registro correspondiente para un resultado.

Los campos de CVSS de interés son:

- Puntuación de CVSS
- Complejidad de acceso
- Impacto de disponibilidad
- Impacto de confidencialidad
- Impacto de integridad
- Autenticación
- Proveedor de acceso
- Origen
- Generado en fecha y hora

Trabajar con pruebas con fallos

Si algunas de las pruebas del asesoramiento muestran un estado fallido, puede realizar una de las acciones siguientes:

Añadir una excepción para la prueba
: Esta acción provoca que se pase la prueba siempre durante un periodo de tiempo. Por ejemplo, es posible que tenga un grupo de servidores que fallan una prueba que comprueba que se han aplicado las últimas actualizaciones de servicio disponibles. No puede aplicar las actualizaciones hasta que se realice la ventana de mantenimiento durante el fin de semana. No desea que la prueba siga fallando hasta ese momento. En el panel de resultados, pulse con el botón derecho del ratón en la palabra Fallo y aparecerá el menú emergente Añadir excepción de prueba. Especifique una fecha y hora de finalización para la excepción y, de forma opcional, un comentario. Se pasará la prueba en todos los orígenes de datos siempre que se ejecute antes de que caduque la excepción, tanto si se ejecuta desde el asesoramiento como si es parte de otro asesoramiento.

Añadir elementos con fallos a un grupo de excepciones
: Cuando una prueba falla, puede visualizar más información pulsando el nombre de la prueba. El nuevo panel incluirá un área denominada Detalles. Los elementos de la prueba que han mostrado fallos se visualizarán tras esta cabecera. Si se visualiza algún elemento, puede añadirlo a un grupo de excepciones de la prueba.

Para ello, pulse la cabecera Detalles: para abrir un nuevo diálogo. Este diálogo visualiza los elementos con fallos, con un recuadro de selección junto a cada uno de ellos. Marque los recuadros de los elementos que desea añadir a un grupo de excepciones y deseleccione los recuadros de selección. A continuación, seleccione un grupo. Si se define un grupo de excepción predeterminado para esta prueba, aparecerá preseleccionado en el diálogo. Una lista desplegable mostrará todos los otros grupos de excepción de prueba de tipo de asesoramiento de vulnerabilidades que se han definido. Para seleccionar un grupo de la lista, pulse el botón de selección junto a la lista y, a continuación, elija el grupo.Haga clic en Guardar para implementar los cambios. Para añadir los elementos restantes a un grupo diferente, vuelva a pulsar Detalles.

Exportar a PDF, o a SCAP o AXIS XML

Puede generar una versión en formato PDF del resultado del asesoramiento pulsando Descargar PDF.

Utilice el botón Descargar XML para abrir dos opciones de menú: Bajar como SCAP xml y Bajar como AXIS xml. Elija una de estas selecciones para poder descargar en su estación de trabajo un archivo XML que represente los resultados del asesoramiento visualizados. El archivo se puede formatear para XML de SCAP (Security Content Automation Protocol) o XML de AXIS (Apache Extensible Interaction System), que utiliza QRadar.

Tema principal: Asesoramientos

Resumen del asesoramiento de vulnerabilidades

La siguiente tabla lista información por prueba y clave de base de datos visualizada en la tabla de resumen asesoramiento de vulnerabilidades: resultado de la prueba por identificador único; antigüedad fallida acumulativa; primera fecha fallida / última fecha fallida; última fecha pasada; y última fecha escaneada. Se realiza un seguimiento de esta información y los usuarios pueden crear un informe sobre la misma.

Resumen de asesoramiento de vulnerabilidades

La clave puede incluir, además de los tres elementos originales, el nombre del origen de datos. El valor predeterminado es un host, puerto y un nombre de instancia.

Utilice el Seguimiento de resúmenes de VA en el Creador de consultas para definir consultas e informes.

Esta tabla se puede exportar e importar. Los datos de importación sustituirán datos existentes en el sistema Guardium (por clave).

Tabla 1. Resumen de VA

Columna de tabla	Tipo	Descripción
VA_SUMMARY_ID	Int	Incrementación automática: clave primaria
DATA_SOURCE_HASH	Varchar(40)	Hash para la clave
DB_TYPE	Varchar	Tipo de base de datos
SERVICE_NAME	Varchar	Nombre de instancia de base de datos (si es parte de la clave, en caso contrario "N/D")
DB_PORT	Varchar	Puerto de base de datos (si es parte de la clave, en caso contrario "N/D")
DB_HOST	Varchar	Host / IP (si es parte de la clave, en caso contrario "N/D")
TEST_ID	Int	ID de la prueba
FIRST_EXECUTION	DateTime	Primera vez que se ejecutó la prueba
LAST_EXECUTION	DateTime	Última vez que se ejecutó la prueba
FIRST_FAIL	DateTime	Primera vez que la prueba falló en esta BD
LAST_FAIL	DateTime	Última vez que la prueba falló en esta BD
FIRST_PASS	DateTime	Primera vez que la prueba se superó en esta BD
LAST_PASS	DateTime	Última vez que se superó la prueba en esta BD
CURRENT_SCORE	varchar	Superado / Fallo / Error
CURRENT_SCORE_SINCE	Datetime	Fecha desde la que la prueba está en el estado actual
CUMULATIVE_FAIL_AGE	Int	Antigüedad fallida acumulativa (en días)
CUMULATIVE_PASS_AGE	Int	Antigüedad pasada acumulativa (en días)

Los mandatos CLI son: store va_test_show_query y show va_test_show_query. Utilice export va_summary para exportar esta información.

Los mandatos GuardAPI para cambiar o visualizar la clave son: grdapi modify_va_summary_key y grdapi reset_va_summary_by_key. El mandato GuardAPI para restablecer la antigüedad acumulativa, tanto la superada como el error, es grdapi reset_va_summary_by_id. Utilice grdapi export_va_summary para exportar esta información.

Se ha añadido un parámetro adicional, datasourceName, a grdapi reset_va_summary_by_key y grdapi modify_va_summary_key.

La entidad de resumen del asesoramiento de vulnerabilidades tiene un atributo adicional, nombre del origen de datos, que se rellena SOLO si el nombre del origen de datos forma parte de la clave.

Nota: El mandato GrdAPI, modify_va_summary_key, permitirá que la clave esté vacía llamando a GrdAPI con los cuatro parámetros: useHost, usePort, useServiceName, useDatasourceName, con el valor false. En ese caso, cuando la clave está vacía, el cálculo del resumen de VA está inhabilitado (no se calcularán, actualizarán ni guardarán los datos de resumen).

Tema principal: Asesoramientos

Cambio de esquema necesario

El esquema que han utilizado las pruebas de asesoramiento de vulnerabilidades en IBM DB2 for z/OS ha cambiado en Guardium V9.1. Si actualiza de una versión anterior a 9.1, deberá actualizar la base de datos para poder continuar utilizando estas pruebas.

Acerca de esta tarea

Cuando actualice el sistema Guardium a la versión 10.x, debe crear nuevas tablas de base de datos en servidor de base de datos. Dichas tablas ofrecen soporte para un nuevo conjunto de pruebas, pero debe crearlas tanto si desea utilizarlas como si no.
En versiones anteriores, creó y completó tablas del esquema gdmmonitor:

- GDMMONITOR.OS_GROUP
- GDMMONITOR.OS_USER

Estas tablas se han sustituido por tablas del esquema CKADBVA:

- CKADBVA.CKA_OS_GROUP
- CKADBVA.CKA_OS_USER

Procedimiento

1. Instalar Guardium 10.x
2. Copie create_CKADBVA-schema_tables_zOS.sql del directorio /var/log/guard/gdmmonitor_scripts en el sistema Guardium en servidor de base de datos. Ejecute el mandato fileserver en servidor de base de datos para recuperar el archivo.
3. El script contiene instrucciones que describen los pasos que se deben llevar a cabo antes de ejecutar el script. Consulte las instrucciones y ejecute el script.
4. Complete las tablas nuevas con datos similares a los datos almacenados en tablas anteriores.

Resultados

El sistema ahora está configurado para utilizar las pruebas de asesoramiento de vulnerabilidades actuales.

Qué hacer a continuación

Tema principal: Asesorar y reforzar

Asesoramiento de vulnerabilidades de RACF

Si utiliza IBM DB2 for z/OS, puede utilizar pruebas de asesoramiento de vulnerabilidades para asesorar las vulnerabilidades de RACF. Debe tener al menos la versión 9.1 de Guardium instalada para utilizar los asesoramientos de RACF.

Acerca de esta tarea

Evalúe los privilegios de RACF (Resource Access Control Facility) tanto si se han concedido en la base de datos como si son externos a ella. Las pruebas, que comprenden los asesoramientos de vulnerabilidades de RACF identifican el control de acceso para los privilegios de objeto, los privilegios de base de datos y los privilegios del sistema.

A fin de utilizar dichas pruebas, debe obtener e instalar zSecure Audit de IBM Security, versión 2.1. Este producto habilita los mandatos que se utilizan en las pruebas para interactuar con RACF.

Las pruebas que examinan titularidades no devuelven un grado pasado/fallo; devuelven una lista de usuarios autorizados. Algunos ejemplos de estos informes incluyen los privilegios de tabla y vista y los privilegios de paquetes concedidos a los receptores de autorización. En un entorno amplio que incluye un gran número de usuarios y aplicaciones, estos informes generan una cantidad de datos abrumadora. Cuando ejecuta estos informes en un entorno tan grande, el proceso puede ejecutarse durante un largo tiempo y consumir grandes cantidades de recursos, por lo que es posible que se agote el tiempo de espera.

Procedimiento

1. Actualice el esquema de base de datos utilizado para dar soporte al asesoramiento de vulnerabilidades en servidor de base de datos.
2. Instale zSecure Audit en servidor de base de datos. Utilice las instrucciones y herramientas que se proporcionan con zSecure Audit para saber cómo llenar aproximadamente 24 tablas en el esquema CKADBVA para dar soporte a las nuevas pruebas de zSecure.
3. El equipo de zSecure emitirá un PTF que permite que zSecure Audit funcione con el asesoramiento de vulnerabilidades de Guardium. Obtenga este PTF y aplíquelo de acuerdo con las instrucciones que lo acompañan.

Resultados

Ahora el sistema está configurado para beneficiarse de las nuevas pruebas de zSecure.

Qué hacer a continuación

Seleccione las nuevas pruebas que desea ejecutar para evaluar las vulnerabilidades de RACF. Configure y ejecute las pruebas.

Tema principal: Asesorar y reforzar

CAS (Configuration Auditing System)

CAS realiza un seguimiento de dichos cambios e informes en ellos. Los datos están disponibles en el sistema Guardium y se puede utilizar para informes y alertas.

Visión general del sistema de auditoría de configuración

Las bases de datos pueden verse afectadas por los cambios en el entorno de servidor; por ejemplo, al modificar los archivos de configuración, las variables de registro o entorno, u otros componentes de base de datos o sistema operativo, incluidos los scripts o los archivos ejecutables que utiliza el sistema de gestión de base de datos o el

sistema operativo. CAS realiza un seguimiento de dichos cambios e informes en ellos. Los datos están disponibles en el sistema Guardium y se puede utilizar para informes y alertas.

Nota: Solo se da soporte al asesoramiento de vulnerabilidades (VA) y a CAS (Configuration Auditing System) en inglés.

Agente CAS

CAS es un agente instalado en el servidor de base de datos e informa al sistema Guardium siempre que se haya modificado una entidad supervisada, ya sea en contenido, en participación o en permisos. Instale un cliente CAS en el sistema de servidor de base de datos, utilizando el mismo programa de utilidad que se ha utilizado para instalar S-TAP. CAS comparte información de configuración con S-TAP, aunque cada componente se ejecuta independientemente del otro. Cuando se haya instalado el cliente CAS en el host, configure las funciones de la auditoría de cambios real desde el portal Guardium.

Servidor CAS

El servidor CAS es un componente de Guardium y se ejecuta en el sistema Guardium. Se ejecuta como un proceso autónomo, independiente del servidor de aplicaciones de Tomcat. Se controla mediante el archivo innittab.

El servidor CAS se configura para utilizar solo algunos procesadores disponibles en el sistema Guardium. El número de procesadores que CAS utiliza se determina utilizando el parámetro *divide_num_of_processors_by*. Este parámetro se almacena en el archivo cas.server.config.properties y su valor predeterminado es 2. Este valor divide el número de procesadores disponibles en el sistema Guardium. Esto garantiza que incluso cuando CAS utiliza el 100% de la CPU en los procesadores asignados, el resto de los procesadores están disponibles para que otras aplicaciones los utilicen.

Autenticación de servidor CAS

Además de la seguridad básica que proporciona SSL, Guardium proporciona soporte de autenticación de servidor CAS en el cliente CAS que se ejecuta en el servidor de base de datos. Esto garantizará que el cliente de CAS se comunique solo con el servidor CAS de Guardium. Las conexiones no autenticadas y los nombres comunes (CN) se notificarán en el archivo de registro de CAS.

Una vez configurado, cuando el servidor CAS se inicia, se cargará un certificado firmado, así como una clave privada, y se asignará a un zócalo de servidor en el que acepta conexiones. En el lado de servidor de base de datos, el cliente CAS dará soporte a las siguientes modalidades de conexión:

1. Conexión no segura (use_tls='0')
2. Conexión segura sin autenticación (use_tls ='1', guardium_ca_path=NULL). Esta modalidad fuerza el uso de SSL como método de comunicación con el servidor CAS (p.ej., utiliza SSL sin la autenticación del servidor).
3. Conexión segura con autenticación de servidor (use_tls ='1', guardium_ca_path=<public key location>). El cliente CAS utiliza la clave pública para autenticar el servidor CAS. La clave pública (ca.cert.pem) se ubicará en <install_dir>/etc/pki/certs/trusted.

   ca.cert.pem: es un archivo que contiene los certificados de entidad emisora de certificados raíz (que se autofirman). En un navegador equivalente, serían los certificados CA de confianza como, por ejemplo, VeriSign, etc.

   La autorización de usuario root emite/firma todos los certificados de gmachine; así es cómo se validan y cómo se establece la cadena de confianza.

   Es posible establecer guardium_ca_path con la vía de acceso completa, incluido el nombre de archivo de claves públicas real, o solo el nombre del directorio (<install_dir>/etc/pki/certs/trusted), en el que se utilizarán todas las claves para autenticar el servidor. Si guardium_ca_path se establece con un archivo o directorio que no contiene la clave pública, el intento de conexión fallará.

4. Conexión segura con autenticación de servidor y verificación de nombre común. Esta modalidad tiene una comprobación adicional en la que el CN del certificado del servidor se compara con el establecido en el parámetro sqlguard_cert_cn. Si sqlguard_cert_cn es nulo o está vacío, la comprobación se inhabilitará. De lo contrario, necesita establecerse con el mismo certificado autofirmado que tiene el CN de Guardium ("gmachine").

Nota: Todos los parámetros mencionados son del archivo guard_tap.ini.

Utilización de SSL con CAS

Puede configurar el agente CAS para que utilice una conexión SSL (Secure Socket Layer) para enviar datos al servidor CAS. El servidor CAS que está instalado con la versión 10.1 cumple con los requisitos del Estándar federal de procesamiento de información 140-2 (FIPS 140-2). Solo un agente CAS conforme con FIPS puede comunicarse con este servidor CAS utilizando SSL. Si desea utilizar este enfoque, deberá actualizar los agentes CAS a la versión entregada con este parche. También debe tener instalado IBM Java en el servidor en el que se ejecuta el agente CAS, y el agente CAS debe estar configurado para utilizarlo. Para poder utilizar la comunicación FIPS, debe estar en uso la autenticación basada en certificados.

Si intenta utilizar un agente CAS antiguo para comunicarse con el servidor CAS actualizado utilizando SSL, verá este mensaje en el archivo de registro en el sistema del agente CAS:

```
javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake_failure
```

Es posible que también vea este mensaje en el archivo de registro CAS en el sistema Guardium

```
javax.net.ssl.SSLHandshakeException: Client requested protocol SSLv3 not
enabled or not supported
```

Si desea utilizar una conexión que no sea SSL entre los agentes CAS y el servidor CAS, puede continuar utilizando los agentes CAS existentes.

Conjunto de plantillas

Un conjunto de plantillas de CAS contiene una lista de plantillas de elementos, agrupadas, que comparten un objetivo común como, por ejemplo, supervisar un tipo de base de datos determinado (Oracle en Unix, por ejemplo); es uno de los dos tipos:

- Solo sistema operativo (Unix o Windows)
- Base de datos (Unix-Oracle, Windows-Oracle, Unix-DB2, Windows-DB2, etc.)

Un conjunto de plantillas siempre es específico para el tipo de base de datos y el tipo de sistema operativo.

Elemento de plantilla CAS

La definición o el conjunto de atributos de una tarea de supervisión sobre una entidad supervisada. Los usuarios pueden definir nuevas pruebas CAS creando unas plantillas CAS, o los usuarios pueden utilizar plantillas CAS predefinidas que se pueden modificar.

Un elemento de plantilla es un archivo o patrón de archivo, un entorno o una variable de registro, la salida de un script SQL o SO, o la lista de usuarios conectados. El estado de cualquiera de estos elementos se refleja mediante datos en bruto, es decir, el contenido de un archivo o el valor de una variable de registro. CAS detecta los cambios comprobando el tamaño de los datos en bruto o calculado una suma de comprobación de datos en bruto. En los archivos, CAS también puede comprobar los cambios a nivel de sistema como, por ejemplo, la propiedad, el permiso de acceso y la vía de acceso de un archivo.

En un entorno federado en el que todas las unidades (recopiladores y agregadores) las gestiona un gestor, los recopiladores y agregadores comparten todas las plantillas y los datos CAS pueden utilizarse en informes o en asesoramientos de vulnerabilidades. Cuando el recopilador y el agregador (o el host en el que se restauran los datos archivados) no forman parte del mismo clúster de gestión, las plantillas no se comparten y, por lo tanto, los asesoramientos de vulnerabilidades no pueden utilizar los datos CAS incluso cuando los datos están presentes. Para solucionarlo, utilice la exportación/importación de definiciones para copiar las plantillas desde el recopilador al agregador (o destino de restauración).

Nota: No se debe pedir a CAS que supervise más de 10.000 archivos por cliente.
Nota: Se recomienda configurar CAS para que no maneje más de 1.000 archivos supervisados por hora.

Entidad supervisada

La entidad actual que se está supervisando puede ser un archivo (su contenido y propiedades), un valor de una variable de entorno o el registro de Windows, la salida de un mandato de SO, un script o una sentencia SQL

Instancia de CAS

Aplicación de un conjunto de plantillas de CAS en un host específico (creando una instancia del conjunto de plantilla y aplicándolo en un host específico)

Configuración de CAS

Una configuración CAS define una o más instancias de CAS. Cada una de ella identifica un conjunto de plantillas que se utilizará para supervisar un conjunto de elementos en dicho host.

Conjuntos de plantillas predeterminadas

Para cada sistema operativo y tipo de base de datos soportada, Guardium proporciona un conjunto de plantillas predeterminadas y preconfiguradas para supervisar una variedad de bases de datos en Unix o en plataformas Windows. Se utilizará un conjunto de plantillas predeterminado como punto de partida para cualquier conjunto de plantillas definido para ese tipo de conjunto de plantillas. Un tipo de conjunto de plantillas es un sistema operativo (Unix o Windows), o un sistema de gestión de base de datos DB2, Informix, Oracle, etc.), que siempre se califica mediante un tipo de sistema operativo, por ejemplo, Oracle para Unix o Windows. Muchos de los conjuntos de plantillas predeterminados y preconfigurados se utilizan en los asesoramientos de vulnerabilidades de Guardium en los que, por ejemplo, se pueden comprobar los parámetros conocidos, las ubicaciones de archivo y los permisos de archivo.

No puede modificar un conjunto de plantillas predeterminado de Guardium, pero puede clonarlo y modificar la versión clonada. Cada conjunto de plantillas predeterminado de Guardium define un conjunto de elementos que se deben supervisar. Asegúrese de que comprende la función y el uso de cada uno de los elementos supervisados por el conjunto de plantillas predeterminado, y utilice los que sean relevantes para su entorno. Después de definir un conjunto de plantillas propio, lo puede designar como predeterminado para este tipo de conjunto de plantillas. Posteriormente, se definirá cualquier conjunto de plantillas definido para este tipo de sistema operativo y de base de datos utilizando el nuevo conjunto de plantillas predeterminado establecido como punto de partida. No se eliminará la plantilla predeterminada de Guardium establecida para este tipo; permanecerá definida, pero no se marcará como predeterminada.

Razón fundamental para crear conjuntos de plantillas para cumplir con las configuraciones de bases de datos específicas

Aunque Guardium proporciona conjuntos de plantillas de CAS predefinidas para cada tipo de base de datos, la amplia variedad de configuraciones de bases de datos posibles significa que es posible que deba ajustar los conjuntos de plantillas predefinidos o crear nuevos para satisfacer sus necesidades en un entorno de producción, especialmente en lo que respecta al software de base de datos y las ubicaciones de archivos de datos. Debe planificar la creación de plantillas adicionales si desea que CAS supervise la propiedad, los permisos y las modificaciones de los archivos de base de datos.

Por ejemplo, el conjunto de plantillas de CAS predefinido para Oracle contiene estas plantillas, entre otras:

- $ORACLE_HOME/oradata/../.*dbf
- $ORACLE_HOME/oradata/../.*ctl
- $ORACLE_HOME/oradata/../.*log
- $ORACLE_HOME/../init.*.ora

Como puede ver, las plantillas de patrón de archivo empiezan con la misma raíz, $ORACLE_HOME (NOTA: Esta no es necesariamente la variable de entorno $ORACLE_HOME definida en su servidor de base de datos; preferentemente, CAS utiliza el campo de origen de datos "Directorio de instancias de bases de datos" como valor para $ORACLE_HOME).

Es posible que en un entorno de producción, los archivos de datos de Oracle no estén en el mismo árbol de directorios, o incluso en el mismo dispositivo que los archivos de registro, y los archivos de configuración de Oracle estén en otra ubicación.

Puede crear plantillas de CAS adicionales utilizando vías de acceso absolutas para permitir que CAS encuentre y supervise todos los archivos de Oracle, por ejemplo:

- /u01/oradata/mydb/*.dbf
- /u02/oradata/mydb/*.dbf
- /u03/oradata/mydb/*.dbf
- /u01/oradata/mydb/*.ctl
- /u02/oradata/mydb/*.ctl
- /u03/oradata/mydb/*.ctl
- /home/oracle11/admin/mydb/bdump/*.log
- /home/oracle11/product/11.1/db_1/dbs/init*.ora

Puede utilizar variables de entorno adicionales definidas en su cuenta de instancia de Oracle. A modo de ejemplo, si tiene variables definidas como $ORA_DATA1, $ORA_DATA2 y $ORA_SOFT, puede utilizar:

- $ORA_DATA1/mydb/*.dbf
- $ORA_DATA2/mydb/*.dbf
- $ORA_DATA1/mydb/*.ctl
- $ORA_DATA2/mydb/*.ctl
- $ORA_SOFT/admin/mydb/bdump/*.log
- $ORA_SOFT/product/11.1/db_1/dbs/init*.ora

Archivos de origen en ubicaciones diferentes

Las plantillas de CAS presuponen que determinados archivos como, por ejemplo, los perfiles de usuarios, se encuentran en ubicaciones específicas. Puede configurar CAS para que busque estos archivos en otras ubicaciones que el usuario especifica utilizando una expresión regular. Para utilizar esta característica, añada el parámetro user_profile_files al archivo cas.client.config.properties en el directorio config. El formato de cada entrada es

identifying_string=lista de archivos separados por comas.

Por ejemplo, supongamos que desea buscar archivos .profile en un directorio de inicio del usuario de DB2. En este ejemplo, presuponemos que los nombres de todos estos directorios de inicio incluyen la cadena "db2".Añada esta línea al archivo de propiedades:

```
user_profile_files=.*db2.*=.profile
```

Si debe especificar más de un patrón, utilice el símbolo de barra (|) para separar patrones. Si desea añadir los perfiles de sus usuarios de mysql a la entrada anterior, sustituya el ejemplo anterior por este:

```
user_profile_files=.*db2.*=.profile|.*mysql.*=.profile
```

- Sustitución por anomalía e inicio de Configuration Auditing System (CAS)
  Pueden modificarse diversos parámetros de conexión y sustitución por anomalía mediante la Auditoría de cambios de Control S-TAP.
- Plantillas de CAS
  Guardium proporciona un conjunto de plantillas de CAS, una para cada tipo de repositorio de datos.
- Cómo trabajar con plantillas de CAS
  En esta sección se describe cómo mantener plantillas de CAS
- Hosts de CAS
  Un host de CAS (Configuration Auditing System) define una o más instancias de CAS.
- Creación de informes de CAS
  Este apartado describe la creación de informes de CAS (Configuration Auditing System).
- Estado de CAS (Configuration Auditing System)
  Abra el Estado de CAS haciendo clic en Gestionar > Supervisión de cambios > Estado de CAS

Tema principal: Asesorar y reforzar

Sustitución por anomalía e inicio de Configuration Auditing System (CAS)

Pueden modificarse diversos parámetros de conexión y sustitución por anomalía mediante la Auditoría de cambios de Control S-TAP.

Cuando se inicia el cliente CAS en el servidor, busca un archivo de punto de comprobación que pueda haber escrito en el sistema. El archivo le muestra a CAS lo que estaba haciendo la última vez que se ejecutó. A continuación, CAS se conecta al sistema Guardium. Si ha encontrado un archivo de punto de comprobación, CAS le pedirá al sistema Guardium verificar la versión de la asignación de supervisión de lo que está almacenado en la base de datos de Guardium. Mientras el cliente CAS y el sistema Guardium estaban desconectados, es posible que se hayan realizado cambios en la asignación. Cuando se resuelvan las diferencias, CAS reanudará la supervisión. Si no encuentra un archivo de punto de comprobación, le preguntará al sistema Guardium lo que debe hacer. Si el sistema Guardium encuentra el host de CAS en la base de datos, se enviarán los conjuntos de plantilla al cliente CAS, se expandirán en los elementos supervisados y se iniciará la supervisión. Si el sistema Guardium no puede encontrar el host de CAS en su base de datos, lo añadirá a la base de datos y enviará el conjunto de plantillas predeterminado para el sistema operativo de host de CAS.

Si se pierde la conectividad entre el cliente de CAS y el sistema Guardium puede que el cliente de CAS y el sistema Guardium necesiten cinco minutos (el tiempo de espera necesario para recibir un mensaje del sistema Guardium) para descubrir que han perdido el contacto con el sistema Guardium primario, pero tomará menos tiempo si se detecta el error de comunicación.

Si el cliente CAS pierde la conexión con el sistema Guardium o no puede realizar una conexión inicial, abrirá un archivo de sustitución por anomalía y empezará a escribir los mensajes que habría enviado al sistema Guardium en el archivo de sustitución por anomalía. La vía de acceso a este archivo de sustitución por anomalía se almacena en guard_tap.ini con el nombre cas_fail_over_file. Cuando se restablece la comunicación, el cliente CAS se cierra y reinicia, envía todos los mensajes almacenados en el archivo de sustitución por anomalía al sistema Guardium y suprime el archivo. Si el cliente de CAS no ha podido establecer la conexión inicial, utilizará el archivo de punto de comprobación para determinar qué debe supervisar, y continuará realizando lo que estaba haciendo antes de que fallara la comunicación.

Si se pierde la comunicación, el cliente iniciará un subproceso que intentará reconectarse periódicamente con el sistema Guardium primario. El número de veces que CAS intentará volver a conectarse y el intervalo de tiempo medio entre los intentos de reconexión son parámetros configurables. Intentará volver a conectarse durante el periodo de tiempo establecido en guard_tap.ini con el nombre cas_server_failover_delay. Una vez transcurrido ese tiempo, también intentará conectarse a servidores secundarios identificados en guard_tap.ini. Los secundarios se probarán en el orden del valor del atributo primario listado en las secciones SQL_Guard de guard_tap.ini. Cuando el primario no es 1, es secundario. Aunque el cliente esté conectado a un servidor secundario, continuará intentado reconectarse al servidor primario.

Si se alcanza el límite de intentos de reconexión, el cliente CAS continua escribiendo datos en un archivo de sustitución por anomalía. Para limitar los requisitos de espacio en el servidor de base de datos, existen dos archivos de sustitución por anomalía. CAS escribe en un archivo hasta que alcanza el tamaño de archivo de sustitución por anomalía máximo (que es configurable) y, a continuación, conmuta al otro, sobrescribiendo los datos anteriores de ese archivo. El tamaño del archivo de sustitución por anomalía predeterminado es 50MB (para cada uno de los archivos).

Puede especificar uno o más sistemas Guardium secundarios al configurar el cliente CAS. En el modo de sustitución por anomalía, CAS solo intenta reconectarse a su servidor primario hasta que se supera el tiempo especificado por cas_server_failover_delay en guard_tap.ini. En ese momento, CAS intenta conectarse a cualquier servidor secundario, además de su servidor primario (que siempre es el primer servidor con el que intenta conectarse durante cualquier intento de reconexión). Aunque esté conectado a un servidor secundario, CAS continuará intentando reconectarse a su servidor primario.

Los cambios en la configuración del cliente CAS solo pueden realizarse desde el servidor primario, mientras el host esté en línea. Siempre que la configuración del cliente CAS se modifique en el servidor primario y el sistema Guardium tenga una configuración autónoma, se guardará un archivo de exportación en el host. Si el cliente CAS se conecta a un servidor secundario, el archivo de exportación guardado se importa desde el host al servidor secundario.

No es necesario mantener por separado las configuraciones en los servidores primario y secundario. Sin embargo, si los parámetros del elemento supervisado individual definidos en la plantilla del servidor primario se han modificado, los cambios no se transferirán al servidor secundario. Por ejemplo, si el valor predeterminado de la plantilla del intervalo de prueba de un archivo determinado se ha cambiado de 1 h a 10 min, el intervalo de prueba del servidor secundario volverá a ser 1 h.Básicamente, los elementos supervisados se vuelven a generar a partir de las plantillas de la configuración importada. El retardo previo a la búsqueda de los servidores secundarios se basa directamente en el tiempo, en lugar del tamaño del archivo de sustitución por anomalía. El retardo se establece con el parámetro cas_server_failover_delay en guard_tap.ini y tiene un valor predeterminado de 60 minutos.

Pueden modificarse diversos parámetros de conexión y sustitución por anomalía mediante la Auditoría de cambios Control S-TAP.

Al igual que con S-TAP, las interrupciones de la conectividad de CAS crean excepciones en el sistema Guardium, por lo que es posible emitir alertas en el momento en que se detecta la interrupción.

Configuración y mantenimiento de servidores secundarios

Es posible definir servidores en el archivo de configuración S-TAP/CAS del sistema de servidor de base de datos de Guardium. Si el servidor primario de Guardium deja de estar disponible, CAS se conectará a un sistema Guardium secundario (tal como se ha descrito anteriormente, consulte Inicio y sustitución por anomalía).

Reglas de la sustitución por anomalía

Núm. regla	Sistema Guardium	Falla en	Válido
1	Autónomo	Autónomo	Sí
2	Gestionado	Gestionado (mismo gestor)	Sí
3	Gestionado	Gestionado (gestor diferente)	No
4	Gestionado	Autónomo	No
5	Autónomo	Gestionado	No

Limitaciones de sustitución por anomalía de CAS

1. Las instancias de CAS no se reubicarán en el sistema Guardium sustituido por anomalía si el sistema Guardium de origen es una unidad gestionada y el sistema Guardium de destino es:
   - un sistema Guardium autónomo
   - una unidad gestionada que está siendo gestionada por un gestor diferente
2. La opción importación/exportación de CAS se limitará únicamente al gestor o a máquinas autónomas.

Exportación de hosts de CAS

1. Pulse Gestionar > Agregación y archivado > Exportar para abrir el panel Exportar definiciones. Seleccione los hosts de CAS en el menú Tipo, seleccione las definiciones a exportar del menú Definiciones para exportar y pulse en Exportar
2. Un archivo denominado exp_<date>_<time>.sql se guardará en el sistema. Este archivo contiene las definiciones de todos los hosts de CAS seleccionados y las definiciones de cualquier conjunto de plantillas que hayan utilizado los hosts de CAS.

Importación de los hosts de CAS

1. Pulse Gestionar > Agregación y archivado > Importar para abrir el panel Importar definiciones.
2. Utilice los botones Examinar y Cargar para seleccionar los archivos y cargarlos y, a continuación, seleccione la definición del panel Importar definiciones subidas.
3. Pulse el icono Importar este conjunto de definiciones para importar la definición.
4. Confirme o no la acción seleccionada.
   Nota: Una operación de importación no sobrescribe la definición existente. Si intenta importar una definición con el mismo nombre que el de una definición existente, se le notificará que el elemento no se ha sustituido. Si desea sobrescribir una definición existente por una importada, debe suprimir la definición existente antes de realizar la operación de importación.

Mantenimiento de servidores secundarios para el host de CAS

Las configuraciones de CAS también se pueden mantener mediante el uso de operaciones de importación y exportación. Puesto que la operación de importación no sustituirá una definición existente, debe suprimir la definición del host de CAS anterior antes de importar una nueva en cada servidor secundario.

Asegúrese de realizar este procedimiento solo mientras el host de CAS seleccionado esté conectado al servidor primario.

1. Exporte la definición del host de CAS (consulte la sección anterior).
2. En cada servidor secundario:
   - Suprima la definición del host de CAS anterior que desea sustituir.
   - Importe las definiciones exportadas del servidor primario (consulte Importación de hosts de CAS).

Instalación del cliente CAS

El agente de cliente CAS se suele instalar junto con el agente S-TAP. Puede instalarse posteriormente en Windows en el DVD de instalación o en Unix ejecutando el script de instalación install_cas.sh, ubicado en el directorio de instalación de S-TAP que, de forma predeterminada, es: /usr/local/guardium/guard_stap.

El cliente CAS ignora alertas de cambios

El cliente CAS puede evitar el envío de notificaciones de cambio al servidor CAS en función de una configuración predefinida.

El agente de cliente CAS ahora buscará un parámetro nuevo ignore_change_alerts en el archivo de configuración cas.client.config.properties del agente de cliente CAS.

Si el parámetro no se encuentra o no se establece, el cliente CAS trabajará sin cambios y la funcionalidad Ignorar alertas de cambio no se habilitará (por ejemplo, el cliente CAS avisará de cualquier cambio de archivo).

Si se establece el nuevo parámetro, el agente de cliente CAS ignorará el envío de notificaciones de cambio en función de los tipos de cambio especificados en el valor de parámetro.

Los tipos de cambio posibles son:

PERMISSION, SIZE, OWNER, GROUP, TIMESTAMP

La concatenación delimitada por + de cualquier tipo de cambio especificado puede establecerse ignorando varios tipos de cambios.

Por ejemplo:

Para evitar el envío de notificaciones de cambio en los cambios OWNER y GROUP, configure el parámetro como se indica a continuación:

ignore_change_alerts=OWNER+GROUP

Nota: El escaneo FIRST de los archivos se realizará en la instalación inicial o al definir la nueva plantilla, y los archivos aparecerán en el informe de cambios de CAS, independientemente de los valores de Ignorar alertas de cambios.

Corrección de un nombre de host sin IP no válido

En el caso de que el usuario instale el agente CAS con los parámetros tap_ip, guard_tap.ini param, o CAS_TAP_IP (parámetro GIM) falsos, es posible que los orígenes de datos de Windows definidos para este servidor no sean útiles (si se utilizan en la actividad que requiere acceder a la base de datos remota).

Si se produce el caso del ejemplo, el usuario tendrá que suprimir los orígenes de datos y modificar el parámetro tap_ip por el nombre de host/ip de servidor de base de datos correcto.

Tema principal: CAS (Configuration Auditing System)

Plantillas de CAS

Guardium proporciona un conjunto de plantillas de CAS, una para cada tipo de repositorio de datos.

Plantillas de CAS: DB2

Script de SO

Designa un script de SO a ejecutar.Debe empezar con la variable $SCRIPTS, que hace referencia al directorio de scripts bajo el directorio de inicio de CAS e identifica el script que va a ejecutar, p. ej., `$HOME/ db2_spm_log_path_group_test.sh"`. El mismo script debe residir en el directorio $SCRIPTS de CAS. La salida del script se almacena en la base de datos de Guardium para que la utilicen los asesoramientos de seguridad.Puede ser un script de shell o por lotes a ejecutar, o un conjunto de mandatos que se pueden especificar en la línea de mandatos. Debido a la naturaleza voluble del análisis de Java, es recomendable que los mandatos más sencillos aparezcan en un script en lugar de ejecutarlos directamente. En Unix, el script se ejecuta en el entorno del usuario de SO especificado. Se definirán tres variables de entorno para cada entorno de ejecución que el usuario puede utilizar para escribir scripts: $UCAS es el nombre de usuario de la BD, $PCAS es la contraseña de la BD y $ICAS es el nombre de instancia de la BD. En Windows estos tres valores se añadirán como los tres últimos argumentos a la ejecución del archivo de procesamiento por lotes.Por ejemplo, si tenía una plantilla de script de SO `%SCRIPTS%\MyScript.bat my-arg1 my-arg2`, %3, %4 y %5 serían el nombre de usuario de la BD, la contraseña y el nombre de la instancia respectivamente.

Archivo

Designa un archivo para que los asesoramientos de seguridad lo rastreen y lo supervisen. La vía de acceso al archivo puede ser absoluta, o relativa a la variable $INSTHOME. Establezca el valor de la variable $INSTHOME en Directorio de instancia de base de datos en el panel Definición de origen de datos. Da nombre a un único archivo. Las variables de entorno del entorno de usuario de SO se pueden utilizar en el nombre de archivo y se ampliarán. Por ejemplo, $HOME/START.sh dará nombre al script de inicio en el directorio de inicio del usuario de DB2.

Patrón de archivo

Designa un archivo para que los asesoramientos de seguridad lo rastreen y lo supervisen. La vía de acceso a los archivos puede ser absoluta, o relativa a la variable $INSTHOME. Establezca el valor de la variable $INSTHOME en Directorio de instancia de base de datos en el panel Definición de origen de datos. .. en la vía de acceso indica uno o más directorios entre la parte de la vía de acceso anterior y la parte de la vía de acceso posterior.El signo .+ en la vía de acceso indica exactamente un directorio entre la parte de la vía de acceso anterior y la parte de la vía de acceso posterior. Por ejemplo: `$INSTHOME/sqllib/../db2.*` es la manera breve de crear muchas identificaciones de archivo único a partir de una única serie de identificación, un patrón de archivo que coincidirá con todos los archivos del directorio.Un patrón de archivo se puede ver como una serie de expresiones regulares separadas por /. Un archivo coincide si cada elemento de su vía de acceso completa puede coincidir con una de las expresiones regulares en orden. Si un elemento del patrón es una variable de entorno, se amplía antes de que empiece la coincidencia. Si .. es uno de los elementos del patrón, coincidirá con cero o más niveles de directorio. Por ejemplo, /usr/local/../foo coincidirá con /usr/local/foo y /usr/local/gunk/junk/bunk/foo. La utilización de más de un elemento .. en un patrón de archivo no debe ser necesario y no se recomienda porque ralentiza la expansión del patrón. Debido a la confusión con su uso en las expresiones regulares, el carácter | no puede utilizarse como separado tal y como se haría en Windows.

Además, el conjunto de asesoramientos Unix/DB2 de Guardium: UNIX - DB2 para Unix incluye las plantillas siguientes:

El bit de modalidad establecer-ID-usuario de Db2govd no se ha establecido

Esta prueba supervisa que se ha desactivado el bit de modalidad establecer-ID-usuario en DB2GOVD

El bit de modalidad establecer-ID-usuario de Db2start no se ha establecido

Esta prueba supervisa que se ha desactivado el bit de modalidad establecer-ID-usuario en DB2START

El bit de modalidad establecer-ID-usuario de Db2stop no se ha establecido

Esta prueba supervisa que se ha desactivado el bit de modalidad establecer-ID-usuario en DB2STOP

Propiedad de archivos

Esta prueba supervisa la propiedad del archivo y los cambios de los archivos de DB2.

Permisos de archivo

Esta prueba supervisa los permisos de archivo de los archivos de DB2.

Plantillas CAS: Informix

Script de SO

Designa un script de SO a ejecutar.Debe empezar con la variable $SCRIPTS, que hace referencia al directorio de scripts bajo el directorio de inicio de CAS e identifica el script que va a ejecutar, p. ej., `$HOME/ informix_rootpath_owner.sh"`. El mismo script debe residir en el directorio $SCRIPTS de CAS. La salida del script se almacena en la base de datos de Guardium para que la utilicen los asesoramientos de seguridad.Puede ser un script de shell o por lotes a ejecutar, o un conjunto de mandatos que se pueden especificar en la línea de mandatos. Debido a la naturaleza voluble del análisis de Java, es recomendable que los mandatos más sencillos aparezcan en un script en lugar de ejecutarlos directamente. En Unix, el script se ejecuta en el entorno del usuario de SO especificado. Se definirán tres variables de entorno para cada entorno de ejecución que el usuario puede utilizar para escribir scripts: $UCAS es el nombre de usuario de la BD, $PCAS es la contraseña de la BD y $ICAS es el nombre de instancia de la BD. En Windows estos tres valores se añadirán como los tres últimos argumentos a la ejecución del archivo de procesamiento por lotes.Por ejemplo, si tenía una plantilla de script de SO `%SCRIPTS%\MyScript.bat my-arg1 my-arg2`, %3, %4 y %5 serían el nombre de usuario de la BD, la contraseña y el nombre de la instancia respectivamente.

Archivo

Designa un archivo para que los asesoramientos de seguridad lo rastreen y lo supervisen. La vía de acceso al archivo puede ser absoluta, o relativa a la variable $INFORMIXDIR. Establezca el valor de la variable $INFORMIXDIR en Directorio de instancia de base de datos en el panel Definición de origen de datos. Da nombre a un único archivo. Las variables de entorno del entorno de usuario de SO se pueden utilizar en el nombre de archivo y se ampliarán. Por ejemplo, $HOME/START.sh dará nombre al script de inicio en el directorio de inicio del usuario de Informix.

Además, el conjunto de asesoramientos de Unix/Informix de Guardium para Unix incluye las plantillas siguientes:

Explorar archivos de registro para detectar errores

Esta prueba supervisa para detectar si hay error en el archivo online.log

Propiedad de archivos

Esta prueba supervisa la propiedad del archivo y los cambios de los archivos de Informix.

Permisos de archivo

Esta prueba supervisa los permisos del archivo y los cambios de los archivos de Informix.

Plantillas de CAS: Oracle

Script de SO

Designa un script de SO a ejecutar.Debe empezar con la variable $SCRIPTS, que hace referencia al directorio de scripts bajo el directorio de inicio de CAS e identifica el script que va a ejecutar, p. ej., $SCRIPTS/oracle_user.sh/. El mismo script debe residir en el directorio $SCRIPTS de CAS. La salida del script se almacena en la base de datos de Guardium para que la utilicen los asesoramientos de seguridad.(Puede ser un script de shell o por lotes a ejecutar, o un conjunto de mandatos que se pueden especificar en la línea de mandatos. Debido a la naturaleza voluble del análisis de Java, es recomendable que los mandatos más sencillos aparezcan en un script en lugar de ejecutarlos directamente. En Unix, el script se ejecuta en el entorno del usuario de SO especificado. Se definirán tres variables de entorno para cada entorno de ejecución que el usuario puede utilizar para escribir scripts: $UCAS es el nombre de usuario de la BD, $PCAS es la contraseña de la BD y $ICAS es el nombre de instancia de la BD. En Windows estos tres valores se añadirán como los tres últimos argumentos a la ejecución del archivo de procesamiento por lotes. Por ejemplo, si tenía una plantilla de script de SO $SCRIPTS/mysql_mysqld_user.sh, %3, %4 y %5 serían el nombre de usuario de la BD, la contraseña y el nombre de la instancia respectivamente.)

Archivo

Designa un archivo para que lo rastreen y supervisen. La vía de acceso al archivo puede ser absoluta, o relativa a la variable $ORACLE_HOME. El valor de la variable de $ORACLE_HOME es el valor que ha establecido en el campo Directorio de instancia de base de datos del panel Definición de origen de datos. (Da nombre a un único archivo. Las variables de entorno del entorno de usuario de SO se pueden utilizar en el nombre de archivo y se ampliarán. Por ejemplo, $HOME/START.sh dará nombre al script de inicio en el directorio de inicio del usuario de Oracle).

Patrón de archivo

Designa un grupo de archivo para que se rastreen y supervisen. La vía de acceso a los archivos puede ser absoluta, o relativa a la variable $ORACLE_HOME. Establezca el valor de la variable $ORACLE_HOME en Directorio de instancia de base de datos en el panel Definición de origen de datos. .. en la vía de acceso indica uno o más directorios entre la parte de la vía de acceso anterior y la parte de la vía de acceso posterior.El signo *.+* en la vía de acceso indica exactamente un directorio entre la parte de la vía de acceso anterior y la parte de la vía de acceso posterior. Por ejemplo: $ORACLE_HOME/oradata/../*.dbf (Es la manera breve de crear muchas identificaciones de archivo único a partir de una serie de identificación única, un patrón de archivo. Un patrón de archivo se puede ver como una serie de expresiones regulares separadas por /. Un archivo coincide si cada elemento de su vía de acceso completa puede coincidir con una de las expresiones regulares en orden. Si un elemento del patrón es una variable de entorno, se amplía antes de que empiece la coincidencia. Si .. es uno de los elementos del patrón, coincidirá con cero o más niveles de directorio. Por ejemplo, /usr/local/../foo coincidirá con /usr/local/foo y /usr/local/gunk/junk/bunk/foo. La utilización de más de un elemento .. en un patrón de archivo no debe ser necesario y no se recomienda porque ralentiza la expansión del patrón. Debido a la confusión con su uso en las expresiones regulares, el carácter \ no puede utilizarse como separado tal y como se haría en Windows. El patrón de archivo mostrado anteriormente no es correcto porque *.dbf no es una expresión regular válida. Debería ser .*dbf.

Además, el conjunto de plantillas de Unix/Oracle de Guardium incluye las siguientes plantillas:

ADMIN_RESTRICTIONS está activado

Esta prueba supervisa si de parámetro listener.ora ADMIN_RESTRICTIONS está activado.

Propiedad de archivos

Esta prueba supervisa la propiedad del archivo y los cambios en los mismos de los archivos de datos, los registros, los ejecutables, etc. de Oracle.

Permisos de archivo

Esta prueba supervisa los permisos del archivo y los cambios en los mismos de los archivos de datos, los registros, los ejecutables, etc. de Oracle.

Explorar archivos de registro para detectar errores

Esta prueba explora los archivos de registro de Oracle en busca de apariciones de series de error.

SPOOLMAIN.LOG no existe

Esta prueba comprueba la existencia de SPOOLMAIN.LOG de Oracle.

Plantillas de CAS: MongoDB

MongoDB se utiliza normalmente como sistema operacional y como programa de fondo para aplicaciones web, debido a la facilidad de programación de los datos con formato no relacionales, como los documentos JSON.

Utilice la plantilla Unix/MongoDB para especificar varias vías de acceso y directorios en el origen de datos para explorar diversos componentes, tal y como se especifica en la definición de origen de datos de MongoDB.

Explore un patrón de archivo seleccionando elementos de plantilla que empiecen por "$".

No seleccione el elemento $SCRIPTS/mongodb_unmask_value.sh ya que es un elemento de reserva de Guardium.

Si el elemento de plantilla no se especifica como parte del Directorio de instancia de base de datos en la definición de origen de datos de MongoDB, el elemento se omitirá y no se explorará.

Nota: Para que los scripts de CAS funcionen, debe habilitar el inicio de sesión para la cuenta de MongoDB en el servidor de BD de Mongo.Para habilitar el inicio de sesión, inicie la sesión como root, ejecute el mandato chsh mongod, y cuando se le solicite el nuevo shell, especifique `/bin/bash`.
Nota: Puede crear su propia plantilla con varias vías de acceso de archivos para cualquier tipo de origen de datos.Al crear su propia plantilla, es recomendable utilizar Unix/MongoDB como referencia. Para crear una nueva plantilla para un origen de datos de MongoDB, puede clonar y modificar la plantilla de Unix/MongoDB.
Nota: Los orígenes de datos de MongoDB soportan conexiones de servidor SSL y cliente/servidor con certificados de cliente de SSL. Las conexiones de MongoDB utilizan un controlador Java en lugar de una conexión de base de datos de JDBC.
Nota: La solución de VA para los clústeres de MongoDB pueden ejecutarse en mongos, un nodo primario y todos los nodos secundarios para conjuntos de réplicas.

Plantillas de CAS: Netezza

Propiedad de archivos

Esta prueba comprueba si se poseen archivos y si pertenecen al grupo correcto de acuerdo con la definición de la plantilla de CAS.

Permiso de archivos

Esta prueba comprueba si el permiso de archivo se ha establecido correctamente de acuerdo con la definición de la plantilla de CAS.

Explorar archivos de registro para detectar errores

Esta prueba comprueba estos sucesos (FATAL, ERROR, DEBUG, ABORT y PANIC) en estos dos archivos de registro. /nz/kit/log/postgres/pg.log y /nz/kit/log/startupsvr/startupsvr.log

Plantillas de CAS: Oracle

Script de SO

Designa un script de SO a ejecutar.Debe empezar con la variable $SCRIPTS, que hace referencia al directorio de scripts bajo el directorio de inicio de CAS e identifica el script que va a ejecutar, p. ej., $SCRIPTS/oracle_user.sh/. El mismo script debe residir en el directorio $SCRIPTS de CAS. La salida del script se almacena en la base de datos de Guardium para que la utilicen los asesoramientos de seguridad.(Puede ser un script de shell o por lotes a ejecutar, o un conjunto de mandatos que se pueden especificar en la línea de mandatos. Debido a la naturaleza voluble del análisis de Java, es recomendable que los mandatos más sencillos aparezcan en un script en lugar de ejecutarlos directamente. En Unix, el script se ejecuta en el entorno del usuario de SO especificado. Se definirán tres variables de entorno para cada entorno de ejecución que el usuario puede utilizar para escribir scripts: $UCAS es el nombre de usuario de la BD, $PCAS es la contraseña de la BD y $ICAS es el nombre de instancia de la BD. En Windows estos tres valores se añadirán como los tres últimos argumentos a la ejecución del archivo de procesamiento por lotes. Por ejemplo, si tenía una plantilla de script de SO $SCRIPTS/mysql_mysqld_user.sh, %3, %4 y %5 serían el nombre de usuario de la BD, la contraseña y el nombre de la instancia respectivamente.)

Archivo

Designa un archivo para que lo rastreen y supervisen. La vía de acceso al archivo puede ser absoluta, o relativa a la variable $ORACLE_HOME. El valor de la variable de $ORACLE_HOME es el valor que ha establecido en el campo Directorio de instancia de base de datos del panel Definición de origen de datos. (Da nombre a un único archivo. Las variables de entorno del entorno de usuario de SO se pueden utilizar en el nombre de archivo y se ampliarán. Por ejemplo, $HOME/START.sh dará nombre al script de inicio en el directorio de inicio del usuario de Oracle).

Patrón de archivo

Designa un grupo de archivo para que se rastreen y supervisen. La vía de acceso a los archivos puede ser absoluta, o relativa a la variable $ORACLE_HOME. Establezca el valor de la variable $ORACLE_HOME en Directorio de instancia de base de datos en el panel Definición de origen de datos. .. en la vía de acceso indica uno o más directorios entre la parte de la vía de acceso anterior y la parte de la vía de acceso posterior.El signo .+ en la vía de acceso indica exactamente un directorio entre la parte de la vía de acceso anterior y la parte de la vía de acceso posterior. Por ejemplo: $ORACLE_HOME/oradata/../*.dbf (Es la manera breve de crear muchas identificaciones de archivo único a partir de una serie de identificación única, un patrón de archivo. Un patrón de archivo se puede ver como una serie de expresiones regulares separadas por /. Un archivo coincide si cada elemento de su vía de acceso completa puede coincidir con una de las expresiones regulares en orden. Si un elemento del patrón es una variable de entorno, se amplía antes de que empiece la coincidencia. Si .. es uno de los elementos del patrón, coincidirá con cero o más niveles de directorio. Por ejemplo, /usr/local/../foo coincidirá con /usr/local/foo y /usr/local/gunk/junk/bunk/foo. La utilización de más de un elemento .. en un patrón de archivo no debe ser necesario y no se recomienda porque ralentiza la expansión del patrón. Debido a la confusión con su uso en las expresiones regulares, el carácter \ no puede utilizarse como separado tal y como se haría en Windows. El patrón de archivo mostrado anteriormente no es correcto porque *.dbf no es una expresión regular válida. Debería ser .*dbf.

Además, el conjunto de plantillas de Unix/Oracle de Guardium incluye las siguientes plantillas:

ADMIN_RESTRICTIONS está activado

Esta prueba supervisa si de parámetro listener.ora ADMIN_RESTRICTIONS está activado.

Propiedad de archivos

Esta prueba supervisa la propiedad del archivo y los cambios en los mismos de los archivos de datos, los registros, los ejecutables, etc. de Oracle.

Permisos de archivo

Esta prueba supervisa los permisos del archivo y los cambios en los mismos de los archivos de datos, los registros, los ejecutables, etc. de Oracle.

Explorar archivos de registro para detectar errores

Esta prueba explora los archivos de registro de Oracle en busca de apariciones de series de error.

SPOOLMAIN.LOG no existe

Esta prueba comprueba la existencia de SPOOLMAIN.LOG de Oracle.

Configuración para sistemas Oracle RAC

Esta es la configuración necesaria para los sistemas Oracle RAC.
Cambie guard_tap.ini en cada nodo instalado con S-TAP:
unix_domain_socket_marker=<key>
donde el valor <key> se puede encontrar en listener.ora en la definición del protocolo IPC
Ejemplo 1:
Si lo siguiente es una descripción en listener.ora
LISTENER=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=ORCL))))
Cambie el parámetro siguiente según corresponda
unix_domain_socket_marker=ORCL
Ejemplo 2:
En caso de que haya más de una línea de IPC en listener.ora, utilice un denominador común en todas las clavesLISTENER=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER)))) LISTENER_SCAN1=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER_SCAN1)))) LISTENER_SCAN2=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER_SCAN2)))) LISTENER_SCAN3=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER_SCAN3))))
Guardium utiliza una búsqueda de serie en la vía de acceso para que LISTENER funcione con las cuatro claves; debería utilizarse en el caso siguiente:
unix_domain_socket_marker=LISTENER

Plantillas de CAS: PostgreSQL

Nota: Es muy importante que las variables de entorno de PostgreSQL_BIN y PostgreSQL_DATA se definan correctamente. Un valor no válido provocará que otras pruebas de asesoramiento de CAS no funcionen correctamente o en absoluto.

Propiedad de archivos

Esta prueba comprueba si se poseen archivos y si pertenecen al grupo correcto de acuerdo con la definición de la plantilla de CAS.

Permiso de archivos

Esta prueba comprueba si el permiso de archivo se ha establecido correctamente de acuerdo con la definición de la plantilla de CAS.

variable de entorno PostgreSQL_BIN definida

Esta prueba comprueba si la variable de entorno de $PostgreSQL_BIN se ha definido en el servidor de base de datos. Esta variable debe definirse en la cuenta raíz de Unix/Linux o puede añadirla a .profile para el inicio de sesión como root. En el SO de Windows, debe definirse para el inicio de sesión de administrador. En Red Hat Linux, la carpeta PostgreSQL BIN es normalmente /usr/bin. En Solaris, por lo general es /data/postgres/postgres/8.3-community/bin/64. El establecimiento de esta variable de entorno es muy importante ya que otras pruebas de asesoramiento se basan en la ubicación de esta carpeta.

variable de entorno de PostgreSQL_DATA definida

Esta prueba comprueba si la variable de entorno de $PostgreSQL_DATA está definida en su servidor de base de datos.Esta variable debe definirse en la cuenta raíz de Unix/Linux o puede añadirla a .profile para el inicio de sesión como root. En el SO de Windows, debe definirse para el inicio de sesión de administrador. En Red Hat Linux, el valor predeterminado de la carpeta DATA es normalmente /var/lib/pgsql/data. No hay ninguna ubicación coherente para Solaris. El establecimiento de esta variable de entorno es muy importante ya que otras pruebas de asesoramiento se basan en la ubicación de dicha carpeta para buscar los archivos de configuración correctos.

Plantillas CAS: Servidor SQL

Script de SO

Designa un script de SO a ejecutar.La salida del script se almacena en la base de datos de Guardium. Puede ser un script de shell o por lotes a ejecutar o un conjunto de mandatos que pueden especificarse en el mandato.

Variable de registro

Busque el registro de Windows para un valor de clave específico necesario para la prueba de asesoramiento de seguridad.

Plantillas CAS: Sybase

Script de SO

Designa un script de SO a ejecutar. Debe empezar con la variable $SCRIPTS, que hace referencia al directorio de scripts bajo el directorio de inicio de CAS e identifica el script que va a ejecutar, p. ej., $HOME/sybase_sysdevice_type_test.sh/. El mismo script debe residir en el directorio $SCRIPTS de CAS. La salida del script se almacena en la base de datos de Guardium para que la utilicen los asesoramientos de seguridad.Puede ser un script de shell o por lotes a ejecutar, o un conjunto de mandatos que se pueden especificar en la línea de mandatos. Debido a la naturaleza voluble del análisis de Java, es recomendable que los mandatos más sencillos aparezcan en un script en lugar de ejecutarlos directamente. En Unix, el script se ejecuta en el entorno del usuario de SO especificado. Se definirán tres variables de entorno para cada entorno de ejecución que el usuario puede utilizar para escribir scripts: $UCAS es el nombre de usuario de la BD, $PCAS es la contraseña de la BD y $ICAS es el nombre de instancia de la BD. En Windows estos tres valores se añadirán como los tres últimos argumentos a la ejecución del archivo de procesamiento por lotes. Por ejemplo, si

tenía una plantilla de script de SO %SCRIPTS%\MyScript.bat my-arg1 my-arg2, %3, %4 y %5 serían el nombre de usuario de la BD, la contraseña y el nombre de la instancia respectivamente.

Archivo

Designa un archivo para que los asesoramientos de seguridad lo rastreen y lo supervisen. La vía de acceso al archivo puede ser absoluta, o relativa a la variable $SYBASE. El valor de la variable de $SYBASE es el valor que ha establecido en el campo Directorio de instancia de base de datos del panel Definición de origen de datos. Da nombre a un único archivo. Las variables de entorno del entorno de usuario de SO se pueden utilizar en el nombre de archivo y se ampliarán. Por ejemplo, $HOME/START.sh dará nombre al script de inicio en el directorio de inicio del usuario de Sybase.

Patrón de archivo

Designa un archivo para que los asesoramientos de seguridad lo rastreen y lo supervisen. La vía de acceso a los archivos puede ser absoluta, o relativa a la variable $SYBASE. El valor de la variable de $SYBASE es el valor que ha establecido en el campo Directorio de instancia de base de datos del panel Definición de origen de datos. .. en la vía de acceso indica uno o más directorios entre la parte de la vía de acceso anterior y la parte de la vía de acceso posterior.El signo .+ en la vía de acceso indica exactamente un directorio entre la parte de la vía de acceso anterior y la parte de la vía de acceso posterior. Por ejemplo: $SYBASE/../.*dat" Es la manera breve de crear muchas identificaciones de archivo único a partir de una única serie de identificación, un patrón de archivo. Un patrón de archivo se puede ver como una serie de expresiones regulares separadas por /. Un archivo coincide si cada elemento de su vía de acceso completa puede coincidir con una de las expresiones regulares en orden. Si un elemento del patrón es una variable de entorno, se amplía antes de que empiece la coincidencia. Si .. es uno de los elementos del patrón, coincidirá con cero o más niveles de directorio. Por ejemplo, /usr/local/../foo coincidirá con /usr/local/foo y /usr/local/gunk/junk/bunk/foo. La utilización de más de un elemento .. en un patrón de archivo no debe ser necesario y no se recomienda porque ralentiza la expansión del patrón. Debido a la confusión con su uso en las expresiones regulares, el carácter \ no puede utilizarse como separado tal y como se haría en Windows.

Además, el conjunto de asesoramientos de Unix/Sybase: UNIX - SYBASE de Guardium incluye las plantillas siguientes:

Explorar archivos de registro para detectar errores

Esta prueba supervisa si hay errores en los archivos de registro de Sybase.

el propietario de sysdevice es sysbase

Esta prueba supervisa la propiedad de sysdevice.

Propiedad de archivos

Esta prueba supervisa la propiedad de archivo y los cambios en los archivos de Sybase.

Permisos de archivo

Esta prueba supervisa los permisos de archivo y los cambios de los archivos de Sybase.

Plantillas de CAS: Teradata

Propiedad de archivos

Esta prueba comprueba si se poseen archivos y si pertenecen al grupo correcto de acuerdo con la definición de la plantilla de CAS.

Permiso de archivos

Esta prueba comprueba si el permiso de archivo se ha establecido correctamente de acuerdo con la definición de la plantilla de CAS.

Aster Data

En 2011, Teradata adquirió Aster Data, que se utiliza normalmente para el depósito de datos y la aplicación de análisis (OLAP). Aster Data creó una infraestructura denominada SQL-MapReduce que permite el uso de SQL (Structured Query Language) con Map Reduce. Aster Data se asocia con más frecuencia a tipos de aplicaciones de secuencia de clics.

Un clúster de Aster, incluye un grupo de nodos Queen, un grupo de nodo de trabajador y un grupo de nodos de cargador. Se instala un agente de CAS en los tres grupos de nodo.

Se debe crear un asesoramiento de seguridad para ejecutar todas las pruebas en el nodo queen. Todas las conexiones de base de datos de Aster Data solo pasan por el nodo queen.

Las pruebas en los nodos de trabajador y de cargador solo son necesarias cuando se realizan pruebas de CAS (permiso de archivo y propiedad de archivo).

Las pruebas de privilegio pasan a través de todas las bases de datos de una instancia determinada.

Al ejecutar pruebas de VA que requieren acceso de CAS y que se rellenen las opciones de configuración del origen de datos de CAS, especifique el nombre de usuario que Aster ha instalado para la cuenta de instancia de base de datos. Este nombre de usuario normalmente se denomina Beehive.

Este es el directorio de inicio del usuario Beehive del directorio de instancias de base de datos. Por lo general, el valor predeterminado es /home/beehive.

Al ejecutar pruebas de VA que no utilizan CAS, el cliente debe crear su origen de datos, apuntando al nodo QUEEN en el clúster.

Al ejecutar pruebas de VA que dependen de CAS, si el nodo que el usuario está probando es el de trabajador, deberá configurar el "URL personalizado" en el origen de datos para que apunte al nodo queen, puesto que es el que está a la escucha.

Ejemplo

Nombre de host/IP = Worker.guard.xxx.xxx..com o 1xx.1xx.111.111 (Es el host de trabajador real aunque el trabajado no esté escuchando. CAS lo necesita para poder enviar y recibir datos del nodo de trabajador)

Puerto = 2046 o cualquiera que sea el puerto utilizado.

Base de datos = beehive

URL personalizado= jdbc:ncluster://aster6q:2406/beehive (Este ejemplo de JDBC muestra que en realidad se está realizando una conexión con aster6q, que es el nodo queen en el puerto 2406 y la base de datos de beehive)

Cuenta de instancia de base de datos = beehive

Directorio de instancia de base de datos = /home/beehive

Tema principal: CAS (Configuration Auditing System)

Cómo trabajar con plantillas de CAS

En esta sección se describe cómo mantener plantillas de CAS

Definir una plantilla o conjunto de plantillas

- Crear un nuevo conjunto de plantillas
- Modificar un conjunto de plantillas
- Clonar un conjunto de plantillas
- Suprimir un conjunto de plantillas

Crear un nuevo conjunto de plantillas

1. Abra el Navegador de configuración de CAS pulsando Reforzar > Control de cambios de configuración (Aplicación CAS) > Configuración del conjunto de plantillas de CAS.
2. Pulse Nuevo para abrir el panel Definiciones de plantillas de elementos supervisados.
3. Seleccione el tipo de SO.
4. Seleccione el tipo de BD. Si el conjunto de plantillas no requiere ningún tipo de BD específico, seleccione N_A como el tipo de BD.
5. Especifique un nombre exclusivo en Nombre de conjunto de plantillas.
   Nota: Los nombres de conjunto de plantillas de más de 128 caracteres se truncarán.
6. Pulse Aplicar para guardar la definición del conjunto de plantillas de CAS.
7. Para añadir elemento al nuevo conjunto de plantillas, pulse Añadir a conjunto y consulte Definir un elemento de conjunto de plantillas.

Búsqueda del panel de CAS de Guardium

De forma predeterminada, el acceso a las funciones de configuración de CAS está restringido al usuario administrador y a los usuarios a los que se ha asignado el rol de CAS.

Pulse Reforzar. La lista de funciones de CAS se lista en la cabecera de Control de cambios de configuración (Aplicación CAS).

Apertura del navegador de configuración de CAS

El panel Navegador de configuración de CAS es el punto de partida para crear o modificar conjuntos de plantillas de CAS.

Abra el panel Navegador de configuración de CAS pulsando Reforzar > Control de cambios de configuración (Aplicación CAS) > Configuración de conjunto de plantillas de CAS.

La lista se puede filtrar por tipo de SO y tipo de BD.

Modificar un conjunto de plantillas

Utilice el panel Navegador de configuración de CAS para modificar un conjunto de plantillas de CAS existente. Cuando un conjunto de plantillas está en uso en cualquier host de CAS, las modificaciones que se pueden realizar al conjunto de plantillas están limitadas. Podrá realizar cambios menores en varios elementos de la definición, pero no podrá añadir ni eliminar plantillas.

1. Abra el panel Navegador de configuración de CAS pulsando Reforzar > Control de cambios de configuración (Aplicación CAS) > Configuración de conjunto de plantillas de CAS.
2. Filtre la lista de conjunto de plantillas por tipo de SO o tipo de BD.
3. Seleccione el conjunto de plantillas que desea modificar y pulse Modificar para abrir el panel Definición del conjunto de plantillas CAS.
4. Realice los cambios que desee y pulse Aplicar para guardarlos.

Clonar un conjunto de plantillas

1. Abra el panel Navegador de configuración de CAS pulsando Reforzar > Control de cambios de configuración (Aplicación CAS) > Configuración de conjunto de plantillas de CAS.
2. Filtre la lista del conjunto de plantillas por tipo de SO o tipo de BD.
3. Seleccione el conjunto de plantillas que desea clonar y pulse Clonar para abrir el panel Definición del conjunto de plantillas CAS.
4. Cuando se haya clonado, modifique la clonación para que se ajuste a sus necesidades.

Nota: Las plantillas predefinidas no se pueden editar. Tienen las mismas restricciones que las que utiliza un host de CAS. El cliente debe clonarlo y editar la copia clonada y desea realizar cambios en la misma.

Suprimir un conjunto de plantillas

1. Abra el panel Navegador de configuración de CAS pulsando Reforzar > Control de cambios de configuración (Aplicación CAS) > Configuración de conjunto de plantillas de CAS.
2. Filtre la lista de conjunto de plantillas por tipo de SO o tipo de BD.
3. Seleccione el conjunto de plantillas que desea suprimir y pulse Suprimir.

Definir un elemento de conjunto de plantillas

Cuando un conjunto de plantillas está en uso en cualquier host de CAS, las modificaciones que se pueden realizar al conjunto de plantillas están limitadas. Podrá realizar cambios menores en varios elementos de la definición, pero no podrá añadir ni eliminar plantillas.

- Crear un elemento de conjunto de plantillas
- Modificar un elemento de conjunto de plantillas
- Suprimir un elemento de conjunto de plantillas

Crear un elemento de conjunto de plantillas

1. Abra el panel Navegador de configuración de CAS pulsando Reforzar > Control de cambios de configuración (Aplicación CAS) > Configuración de conjunto de plantillas de CAS.
2. Pulse Nuevo para abrir el panel Definiciones de plantillas de elementos supervisados.
3. Entre en un Nombre de conjunto de plantillas, seleccione tipo de SO y tipo de BD y pulse Aplicar.
4. Seleccione Añadir a conjunto para crear un elemento nuevo.

Modificar un elemento de conjunto de plantillas

1. Abra el panel Navegador de configuración de CAS pulsando Reforzar > Control de cambios de configuración (Aplicación CAS) > Configuración de conjunto de plantillas de CAS.
2. Filtre la lista de conjunto de plantillas por tipo de SO o tipo de BD.
3. Seleccione el conjunto de plantillas que desea modificar y pulse Modificar para abrir el panel Definición del conjunto de plantillas CAS.
4. Seleccione los elementos que desea modificar y pulse Editar seleccionados.... Realice los cambios que desee y pulse Aplicar para guardarlos.

Suprimir un elemento de conjunto de plantillas

1. Abra el panel Navegador de configuración de CAS pulsando Reforzar > Control de cambios de configuración (Aplicación CAS) > Configuración de conjunto de plantillas de CAS.
2. Filtre la lista de conjunto de plantillas por tipo de SO o tipo de BD.
3. Seleccione el conjunto de plantillas que desea modificar y pulse Modificar para abrir el panel Definición del conjunto de plantillas CAS.
4. Seleccione los elementos que desea suprimir y pulse Suprimir seleccionados.

Panel de definición de la plantilla de elemento de CAS

Componente	**Descripción**
Tipo de SO	El tipo de sistema operativo: Windows o Unix. Puede cambiar esta selección cuando el conjunto de plantillas esté vacío, pero no puede modificarlo si el conjunto de plantillas contiene uno o más elementos.
Tipo de BD	El tipo de base de datos (Oracle, MS-Sqlm DB2, Sybase, Informix, etc.) o N/D para un conjunto de plantillas del sistema operativo. Puede cambiar la selección cuando el conjunto de plantillas esté vacío, pero no puede modificarlo si contiene uno o más elementos.
Descripción	Un nombre opcional para el elemento utilizado en los informes y para identificar el elemento en otros paneles de CAS (Definición del conjunto de plantillas CAS, por ejemplo). Si se omite, el nombre del elemento toma de forma predeterminada el nombre de archivo o patrón, el nombre de variable o el script (según corresponda para el tipo).
Tipo	Uno de los siguientes: consulta SQL, script de SO, variable de entorno, variable de registro, patrón de variable de registro, archivo y patrón de archivo. Consulte Tipos de auditoría y plantilla para obtener más información. Nota: Si se está utilizando con pruebas de asesoramiento basadas en CAS, debe ser el tipo de script de SO.
Contenido	Escriba el texto dependiente que defina el elemento específico a supervisar, o cómo generarlo. Consulte Tipos de auditoría y plantilla para obtener más información. Nota: Para un script de SO, CAS esperará a que se complete un script. Utilice el parámetro cas_command_wait guard_tap.ini para limitar el tiempo permitido para que un script de SO se ejecute y permita que el CAS termine el script. El tiempo de espera predeterminado es 300 segundos o 5 minutos. Cuando cambie este parámetro, no es necesario que reinicie CAS.
Límite de permiso	Solo en los archivos y tipos de patrón de archivo. Utilizado solo en Unix: los permisos que este archivo no debería superar.
Propietario del archivo	Solo en los archivos y tipos de patrón de archivo. El propietario de los archivos.
Grupo de archivos	Solo en los archivos y tipos de patrón de archivo. El propietario de grupo de los archivos.
Período	El intervalo máximo entre pruebas, especificadas como un número de minutos (m), horas (h) o días (d). Los datos están disponibles una vez cumplido el período inicial y antes de que empiece el período siguiente.
Conservar datos	Si se selecciona, se guardará una copia de los datos reales con cada cambio. Por ejemplo: para un elemento de archivo, se guarda una copia del archivo. Si se selecciona, pero el tamaño de los datos sin formato del elemento es mayor al Límite de datos en bruto configurados para el host de CAS, no se guardarán los datos.

Uso de MD5	Indica si la comparación se realiza o no mediante el cálculo de la suma de comprobación de los datos sin formato utilizando el algoritmo MD5. El cálculo de la suma de comprobación MD5 consume tiempo de los objetos de caracteres grandes. Sin embargo, es mejor indicador de cambio que el tamaño. El valor predeterminado es no utilizar MD5. Si se utiliza el MD5, pero el tamaño de los datos sin formato es mayor que el Límite de tamaño de MD5 configurado para el host de CAS, se omitirán el cálculo y la comparación de MD5.
Habilitado	Se selecciona de forma predeterminada; indica si se comprobará si hay cambios en el elemento o no.

Tipos de auditoría de plantilla

Tipo	Descripción
Consulta SQL	El contenido debe ser una sentencia SQL válida. El resultado devuelto por la sentencia se comparará con el resultado devuelto la última vez que se ejecutó la consulta. La consulta se ejecutará con los parámetros especificados en el origen de datos que se está utilizando: nombre de usuario, contraseña, puerto de BD, etc. Se debe tener cuidado al rellenar estos parámetros en el origen de datos o la consulta no podrá devolver el resultado.
Script de SO	El contenido puede ser una entrada de línea de mandatos válida o el nombre de un archivo que contenga un script ejecutable de SO. El script se ejecuta en el entorno del usuario de SO especificado en el campo Cuenta de instancia de base de datos de la definición de origen de datos.
Variable de entorno	El contenido debe nombrar una variable de entorno definida en el contexto del usuario de SO especificado en el campo Cuenta de instancia de base de datos de la definición de origen de datos.
Variable de registro	El contenido se interpreta como la vía de acceso a una variable en el registro de Windows del host. El valor encontrado en dicha vía de acceso se compara con el valor encontrado la última vez que se rastreó la vía de acceso.
Patrón de variable de registro	El contenido es una secuencia de expresiones regulares que se utiliza para que coincida con los componentes de las vías de acceso en el registro de Windows. El patrón se utiliza para desarrollar elementos supervisados de tipo de variable de registro que se tratarán como se ha descrito anteriormente. Las expresiones regulares se unen mediante / para que el patrón se asemeje a una vía de acceso del registro. El carácter |, más familiar, no se puede utilizar ya que se trata de un carácter especial en la sintaxis de las expresiones regulares de Java™. Si se necesita el carácter / en alguna de las expresiones regulares, debe usarse |. (p. ej. se utilizaría U\/235 para que coincidiera con U/235). El patrón .. se puede utilizar para que coincida con cero o más componentes en una vía de acceso. Por ejemplo, HKLM/Software/../buzz coincidirá con HKLM\Software\buzz, o HKLM\Software\uno\dos\tres\buzz. Este tipo de patrón puede llevar a una búsqueda de registros costosa, por lo que debe utilizarlo con cuidado. Además de estas excepciones, las expresiones regulares siguen la sintaxis de las expresiones regulares de Java.
Archivo	El contenido se interpreta como una vía de acceso de archivo absoluta en el sistema principal. Las características del archivo encontrado en la vía de acceso se compararán con la característica encontrada la última vez que se creó la vía de acceso. La vía de acceso incluye variables de entorno que se ampliarán en el contexto del usuario de SO especificado en el origen de datos. La vía de acceso también puede empezar con una variable de sustitución, como "$SYBASE_HOME", que se sustituirá por el valor especificado en el campo Directorio de instancia de base de datos de la definición de origen de datos.
Patrón de archivo	El contenido es una secuencia de expresiones regulares que se utiliza para que coincida con los componentes de vías de acceso de archivos y para generar elementos supervisados de tipo de archivo. Las expresiones regulares están unidas por el carácter /, por lo que el patrón se asemeja a una vía de acceso de archivo real. Al igual que con los patrones de registro, el carácter | no se puede utilizar en los archivos de Windows debido a la sintaxis de la expresión regular. Si el patrón empieza con *?:* en una máquina de Windows, la coincidencia de patrón se iniciará en cada una de las unidades de una máquina con varias unidades. La construcción .. descrita con los patrones de registro también se puede utilizar en un patrón de archivo. Las variables de entorno del contexto del usuario de SO se pueden utilizar en un patrón de archivo y se ampliarán antes de la expansión de las expresiones regulares.

mandatos GuardAPI

create_cas_template_set

create_cas_template

create_datasource

create_cas_host_instance

Tema principal: CAS (Configuration Auditing System)

Hosts de CAS

Un host de CAS (Configuration Auditing System) define una o más instancias de CAS.

Una vez haya definido uno o más conjuntos de plantillas de CAS y haya instalado CAS en un servidor de base de datos, podrá configurar CAS en dicho host. Una configuración de host de CAS define una o más instancias de CAS. Cada instancia especifica un conjunto de plantillas de CAS y define cualquier parámetro necesario para conectarse a la base de datos. Para cada servidor de base de datos en el que está instalado el CAS, existe una configuración de host de CAS única que normalmente contiene varias instancias de CAS, por ejemplo, una instancia de CAS para supervisar elementos de sistema operativo, instancias de CAS adicionales para supervisar elementos del sistema operativo e instancias de CAS adicionales para supervisar instancias de base de datos individuales.

- Definir una instancia de CAS
- Modificar una instancia de CAS
- Suprimir una instancia de CAS
- Inhabilitar una instancia de CAS

Definir una instancia de CAS

1. Abra el Navegador de configuración de CAS pulsandoReforzar > Control de cambios de configuración (Aplicación CAS) > Configuración de host de CAS.

   El menú lista todos los servidores de base de datos en los que se ha instalado CAS, y el host se ha conectado al sistema Guardium.

2. Utilice el filtrado de lista para filtrar por tipo de SO o tipo de BD y busque el host con el que desea trabajar.
3. Resalte el host que desea modificar y pulse Modificar.
4. Seleccione un conjunto de plantillas en el menú.
   Nota: La instancia de CAS no puede definirse si el host está fuera de línea o se trata de un sistema Guardium secundario para el host.
5. Pulse Añadir origen de datos para abrir el panel Buscador de orígenes de datos.
   Nota: Si no hay ningún origen de datos compatible para el conjunto de plantillas del host, puede pulsar Nuevo para abrir el panel Definición de origen de datos y añadir un origen de datos.
6. Seleccione el origen de datos que desea añadir al conjunto de plantillas y pulse Añadir para añadirlo al conjunto de plantillas.

Búsqueda del panel de CAS de Guardium

El acceso a las funciones de configuración de CAS está restringido al administrador y a los usuarios a los que se ha asignado el rol de CAS.

Pulse Reforzar. Todas las funciones de CAS se listan en la cabecera Control de cambios de configuración (Aplicación CAS).

Abra el navegador de configuración de CAS

El panel Navegador de configuración de CAS es el punto de inicio para crear o modificar hosts de CAS.

Abra el panel Navegador de configuración de CAS pulsando Reforzar > Control de cambios de configuración (Aplicación CAS) > Configuración de host de CAS.

Modificar una instancia de CAS

1. Abra el Navegador de configuración de CAS
2. Utilice el filtrado de listas para filtrar por tipo de SO o tipo de BD y buscar la instancia con la que desea trabajar.
3. Resalte el host que desea modificar y pulse Modificar.

   Se visualizará una lista de las instancias de CAS definidas asociadas al host seleccionado con la información y las opciones de edición siguientes:

Tabla 1. Modificar una instancia de CAS

Componente	Descripción
Icono de instancia habilitar/inhabiltar	Pulse el icono Inhabilitar instancia para inhabilitar/habilitar la instancia de CAS
Icono de instancia Suprimir	Pulse el icono Suprimir instancia para suprimir la instancia de CAS
Origen de datos	Identifica el origen de datos que ha utilizado la instancia. Pulse **Origen de datos** para abrir el panel Definición de origen de datos y editar la definición de origen de datos
Conjunto de plantillas	Identifica el conjunto de plantillas de CAS utilizado por la instancia. Pulse este enlace para abrir el panel Definiciones de plantillas de elementos supervisados y visualizar o modificar la definición de conjunto de plantilla. Consulte Cómo trabajar con plantillas de CAS para obtener más información
Elementos supervisados	Un recuento de elementos que la instancia está supervisando. Pulse el enlace para abrir el panel Definiciones de elementos supervisados, que muestra la lista de todos los elementos que se están supervisando actualmente. Consulte Visualización de listas de elementos supervisados para obtener más información. Nota: Hay un valor predeterminado de 10.000 elementos supervisados visibles en los informes, independientemente del número de elementos supervisados definidos. Es recomendable definir varias instancias cuando el número de elementos supervisados se aproxima al límite.

Suprimir una instancia de CAS

1. Abra el Navegador de configuración de CAS
2. Utilice el filtrado de listas para filtrar por tipo de SO o tipo de BD y buscar la instancia con la que desea trabajar.
3. Pulse Suprimir instancia para suprimir una instancia de CAS. También se suprimirán todos los datos de cambio recopilados.

Inhabilitar una instancia de CAS

1. Abra el Navegador de configuración de CAS.
2. Utilice el filtrado de listas para filtrar por tipo de SO o tipo de BD y buscar la instancia con la que desea trabajar.
3. Resalte el host que desea modificar y pulse Modificar, o haga doble clic para abrir el panel Definiciones de instancia de host.
4. Pulse el icono Inhabilitar instancia para inhabilitar la instancia de CAS. Los datos de cambio no se recopilarán hasta que se habilite la instancia pulsando el icono.

Ver listas de elementos supervisados

En el panel Definiciones de instancia de host, pulse el enlace Elementos supervisados para visualizar la lista completa de elementos supervisados en el panel Definiciones de elementos supervisados. La tabla siguiente describe los componentes vistos en el panel Definiciones de elementos supervisados para esta configuración de host.

Todos los elementos supervisados hacen referencia a datos sin formato, un objeto de carácter en el host, el resultado de una consulta SQL, la salida de un script de SO o el contenido de un archivo. Se calculará el tamaño del objeto de carácter. Si el elemento es un archivo, los permisos, el propietario, el grupo y la hora de la última modificación también se comprueban. Si alguno de los anteriores ha cambiado desde la última vez que se comprobó el elemento, se anotará el cambio.

Tabla 2. Ver listas de elementos supervisados

Componente	Descripción
Recuadro de selección	Seleccione el recuadro de selección si desea editar un elemento supervisado individualmente o como grupo. Haga doble clic en cualquier elemento supervisado para editar dicho elemento.
Elemento	El nombre del elemento supervisado de la descripción en el panel Definición de plantillas de elementos CAS
Tipo	Uno de los siguientes: Script de SO, consulta SQL, archivo, variable de entorno o variable de registro Script de SO o Script SQL: El texto real o la vía de acceso a un script de sistema operativo o SQL, cuya salida se comparará con la salida producida la próxima vez que se ejecute Archivo o patrón de archivo: Un archivo específico o un patrón para identificar un conjunto de archivos Variable de entorno o variable de registro: Una variable de entorno o una variable de registro (Windows)
Período	El intervalo promedio entre pruebas, que se muestra en forma de número en segundos (s), minutos (m), horas (h) o días (d).
Conservar datos	Si se marca, se guardará una copia de los datos reales con cada cambio. Por ejemplo, para un elemento de archivo, se guarda una copia del archivo. Si se marca, pero el tamaño de los datos en bruto para el elemento es mayor que el límite de datos en bruto configurado para este host de CAS, no se guardarán los datos
Uso de MD5	Indica si la comparación se realiza o no mediante el cálculo de la suma de comprobación de los datos sin formato utilizando el algoritmo MD5. El cálculo de la suma de comprobación MD5 consume tiempo de los objetos de caracteres grandes. Sin embargo, es mejor indicador de cambio que el tamaño. El valor predeterminado es no utilizar MD5. Si se utiliza MD5 pero el tamaño de los datos a tratar es mayor que el límite de tamaño de MD5 configurado para el host de CAS, el cálculo y la comparación MD5 se omitirán.

Mandatos GuardAPI

delete_cas_host

list_cas_hosts

create_cas_host_instance

delete_cas_host_instance

list_cas_host_instances

update_cas_host_instance

Tema principal: CAS (Configuration Auditing System)

Creación de informes de CAS

Este apartado describe la creación de informes de CAS (Configuration Auditing System).

El usuario administrador tiene acceso a todos los creadores de consultas e informes predeterminados. El rol de administrador permite el acceso a los informes CAS predeterminados, pero no a los editores de consultas de CAS. El rol CAS permite el acceso a los informes CAS predeterminados y a los creadores de consultas.

- Acceso a los creadores de consultas de CAS
- Acceso a informes de CAS predeterminados
- Dominios de creación de informes de CAS

Acceso a los creadores de consultas de CAS

Esta sección describe cómo acceder a los creadores de consultas de CAS desde los portales de usuario y de administrador. Para obtener ayuda acerca de cómo utilizar los creadores de consultas o de informes, vaya a Consultas o Informes.

Desde la IU:

1. Abra el Creador de informes haciendo clic en Investigar > Creador de informes.
2. Pulse Nuevo, seleccione Consulta del menú, especifique un título de informe, pulse Siguiente, y rellene el resto de los campos del Creador de informes para que se ajuste a sus necesidades.

Acceso a informes de CAS predeterminados

Visualice los informes predeterminados relacionados con CAS pulsando Reforzar > Informes.

Dominios de creación de informes de CAS

Dominio	Descripción
Plantillas de CAS	Realice el seguimiento de las definiciones de plantilla de CAS. Las plantillas identifican los elementos que se van a supervisar para los cambios. Los elementos supervisados pueden ser archivos, variables de entorno o de registro, conjuntos de salida de script SQL o de SO o conjuntos de usuarios conectados.
Configur	Realiza un seguimiento de las configuraciones de host de CAS, en las que una configuración es la aplicación de uno o más conjuntos de plantillas a un host de

ación de CAS	servidor de base de datos específico. En las instancias de configuración puede visualizar qué elementos de los conjuntos de plantillas están habilitados o inhabilitados, o qué archivos seleccionan y supervisan (o no) las plantillas de patrón de nombre de archivo.
Historial de hosts de CAS	Realiza un seguimiento de los sucesos de host de CAS, incluidos los servidores o los clientes que están fuera de servicio.
Cambios de CAS	Realiza un seguimiento de las modificaciones realizadas en los elementos supervisados (archivos, variables de registro, etc.)

Dominio de plantillas de CAS

Entidad	Descripción
Conjunto de plantillas	Describe una definición de conjunto de plantillas
Plantilla	Describe un elemento de plantilla dentro de un conjunto de plantillas

Entidad Conjunto de plantillas

Atributo	Descripción
ID de conjunto de plantillas	Un identificador exclusivo para el conjunto de plantillas, numerado secuencialmente
Tipo de SO	Sistema operativo: Unix o Windows
Tipo de BD	Tipo de base de datos (Oracle, MS-SQL, DB2, Sybase, Informix, etc.) o N/D para una plantilla de sistema operativo
Nombre de conjunto de plantillas	El nombre de la plantilla
Predeterminado	Indica si la plantilla es o no la predeterminada para la combinación de tipo de SO especificado y el tipo de BD
Editable	Indica si se puede modificar o no la plantilla. Las plantillas predeterminadas de Guardium no se pueden modificar.Además, una vez se ha utilizado un conjunto de plantillas en una instancia de CAS, no se puede modificar. Sin embargo, un conjunto de plantillas siempre se puede clonar y el conjunto clonado se puede modificar.
Indicación de fecha y hora	Fecha y hora en que se actualizó la plantilla

Entidad Plantilla

Atributo	Descripción
ID de plantilla	Un identificador exclusivo para el conjunto de plantillas, numerado secuencialmente
Nombre de acceso	En función del tipo de auditoría, se trata del SO o del script SQL, entorno o valor de registro, o un nombre de archivo o un patrón de nombre de archivo
Tipo de auditoría	El tipo de elemento supervisado
Frecuencia de auditoría (minutos)	El intervalo máximo (en minutos) entre pruebas
Utilizar MD5	Indica si la comparación se realiza o no calculando una suma de comprobación utilizando el algoritmo MD5 y comparando dicho valor con el valor calculado la última vez que se comprobó el elemento. El valor predeterminado es no utilizar MD5. Si se utiliza MD5 pero el tamaño de los datos a tratar es mayor que el Límite de tamaño de MD5 configurado para el host CAS, se omitirá el cálculo y la comparación MD5. Independientemente de si se utiliza o no MD5, tanto el valor actual de la indicación de fecha y hora de la última modificación para el elemento y el tamaño del elemento se comparan con los valores que se han guardado la última vez que se comprobó el elemento.
Guardar datos	Indica si se ha marcado el recuadro de selección Conservar datos. Si es así, las versiones anteriores del elemento pueden compararse con la versión actual.
Descripción	Descripción opcional de la plantilla
Indicación de	Fecha y hora en que se actualizó la plantilla.

fecha y hora	

Informes predeterminados de dominio de plantillas de CAS

Informe predeterminado	Descripción
Informe de plantilla de CAS	Lista las plantillas de CAS

Informe de plantilla de CAS

Entidad	Atributo	Operador	Valor predeterminado
Plantilla	Access_Name	Como	%
Conjunto de plantillas	Template_Set_Name	Like	%
Plantilla	Audit_Type	Like	%

Dominio de configuración CAS

Entidad	Descripción
Host	Identifica un host de CAS (un servidor de base de datos) y el estado actual de CAS (en línea/fuera de línea). Esta entidad también está disponible en el dominio Historial de hosts de CAS
Configuración de instancia	En cada host, una entrada de configuración de host describe una instancia de CAS que contiene parámetros de conexión de base de datos (si son necesarios) e identifica el conjunto de plantilla que utiliza la instancia. Proporciona el estado actual de la última instancia (en uso, habilitada o inhabilitada) y la fecha de la última revisión.
Detalles de elemento supervisado	Identifica un elemento (un archivo o una variable de entorno, por ejemplo) supervisado por una instancia CAS. Contiene la definición de elemento e indica si el elemento está habilitado o no.

Entidad Host

Entidad	Descripción
Nombre de host	Nombre de host del servidor de bases de datos (se puede mostrar como una dirección IP)
Tipo de SO	Sistema operativo: UNIX o WIN
Está en línea	Estado en línea (sí o no) cuando se grabó el registro

Entidad Configuración de instancia

Atributo	Descripción
Tipo de BD	Tipo de base de datos (Oracle, MS-SQL, DB2, Sybase, Informix, etc.) o N/D para una instancia de sistema operativo
Instancia	Nombre de la instancia.
Usuario	Nombre de usuario que CAS utiliza para iniciar una sesión en la base de datos o N/D para una instancia de sistema operativo.
Puerto	El número de puerto utiliza CAS para conectarse a la base de datos; puede estar vacío para una instancia de sistema operativo
Directorio inicio BD	El directorio de inicio de la base de datos; puede estar vacío para una instancia de sistema operativo
ID de conjunto de plantillas	Identifica el conjunto de plantillas utilizado por esta instancia

Entidad Detalles del elemento supervisado

Atributo	Descripción
ID de plantilla	Tipo de base de datos (Oracle, MS-SQL, DB2, Sybase, Informix, etc.) o N/D para una instancia de sistema operativo
Elemento supervisado	Nombre de la instancia.
Tipo de auditoría	Nombre de usuario que CAS utiliza para iniciar una sesión en la base de datos o N/D para una instancia de sistema operativo.

Habilitado	El número de puerto utiliza CAS para conectarse a la base de datos; puede estar vacío para una instancia de sistema operativo
En sincronización	El directorio de inicio de la base de datos; puede estar vacío para una instancia de sistema operativo
Frecuencia de auditoría	Identifica el conjunto de plantillas utilizado por esta instancia
Utilizar MD5	Indica si la comparación se realiza o no calculando una suma de comprobación utilizando el algoritmo MD5 y comparando dicho valor con el valor calculado la última vez que se comprobó el elemento. El valor predeterminado es no utilizar MD5. Si se utiliza MD5 pero el tamaño de los datos a tratar es mayor que el Límite de tamaño de MD5 configurado para el host CAS, se omitirá el cálculo y la comparación MD5. Independientemente de si se utiliza o no MD5, tanto el valor actual de la indicación de fecha y hora de la última modificación para el elemento y el tamaño del elemento se comparan con los valores que se han guardado la última vez que se comprobó el elemento.
Guardar datos	Cuando se marca, la versión anterior del elemento se puede comparar con la versión actual
Descripción	Descripción opcional de la instancia
Contenido de plantilla	Entrada de plantillas que es la base para este elemento supervisado, establecido desde el atributo Nombre de acceso de la entidad Plantilla cuando se creó la instancia. Normalmente será el mismo que el elemento supervisado, pero en el caso de que se haya utilizado un patrón de archivo en la plantilla, éste será el patrón de archivo.

Informes predeterminados de dominio de configuración de CAS

Informes predeterminados	Descripción
Instancias de CAS	Lista instancias de CAS
Configuración de instancias de CAS	Lista las modificaciones de la configuración de instancias de CAS

Informe de instancias de CAS

Entidad	Atributo	Operador	Valor predeterminado
Host	Host_Name	Like	%
Host	OS_Type	Like	%
Configuración de instancia	DB_Type	Like	%
Configuración de instancia	Instancia	Like	%

Informe de configuración de instancias de CAS

Entidad	Atributo	Operador	Valor predeterminado
Host	Host_Name	Like	%
Host	OS_Type	Like	%
Detalles de elemento supervisado	Template_Id	Like	%

Informes detallados

Informe	Descripción
Detalles de informe	Muestra los elementos supervisados incluidos en el recuento de columnas de elementos supervisados

Dominio de historial de host de CAS

Lista de entidades	Descripción de dominio
Host	Identifica un host de CAS (un servidor de base de datos) y el estado actual de CAS (en línea/fuera de línea). Esta entidad también está disponible en el dominio de configuración de CAS.
Suceso de host	La fecha y hora de un suceso en la relación de cliente/servidor de CAS detalla un cliente o un servidor que está dentro y fuera del servicio.

Entidad Host

Atributo	Descripción
Nombre de host	Nombre de host del servidor de base de datos
Tipo de SO	Sistema operativo: Unix o Windows
Está en línea	Estado de conexión actual (Sí/No)

Suceso de host

Atributo	Descripción
Hora de suceso	Fecha y hora en que se registró el suceso
Tipo de suceso	Identifica el suceso que se está registrando: "Cliente inactivo": CAS detenido en el host de servidor de base de datos "Cliente activo": CAS iniciado en el host de servidor de base de datos "Sustitución por anomalía inactiva": Hay disponible un servidor (que sigue a una interrupción), de forma que los datos de CAS se están escribiendo en el servidor "Sustitución por anomalía activa": El servidor no está disponible, por lo que los datos de CAS se están escribiendo en el archivo de sustitución por anomalía "Servidor inactivo": El servidor de bases de datos se ha detenido "Servidor activo": Se ha iniciado el servidor de bases de datos

Informes predeterminados de dominio de historial de CAS

Informe predeterminado	Descripción
Informe de historial de host de CAS	Lista los sucesos de CAS para cada host de CAS

Informe de historial de host de CAS

Entidad	Atributo	Operador	Valor predeterminado
Host	Host_Name	Like	%
Host	OS_Type	Like	%
Suceso de host	Event_Type	Like	%

Dominio de cambios de CAS

Entidad	Descripción
Cambios supervisados	Se crea cada vez que se modifica un elemento supervisado
Configuración de host	Se crea cada vez que se modifica un elemento supervisado
Datos guardados	Contiene datos guardados de los cambios realizados

Entidad Cambios supervisados

Atributo	Descripción
Identificador de cambio	Identificador exclusivo del cambio
Tiempo de muestreo	Indicación de fecha y hora (fecha y hora del host) en que se ha tomado la muestra
ID de datos guardados	Identifica la entidad Datos guardados para este cambio
ID de etiqueta de estado de auditoría	Identifica la entidad de Configuración de host para este cambio
Indicación de fecha y hora	Fecha y hora en que se creó el registro de cambios en el servidor (reloj de servidor de dispositivo de Guardium)
Propietario	Solo en UNIX. Si el tipo de elemento es un archivo, el propietario del archivo.
Permisos	Solo en UNIX. Si el tipo de elemento es un archivo, los permisos del archivo.
Tamaño	El tamaño de archivo, con los siguientes valores especiales: -1, El archivo existe, pero contiene cero bytes 0, El archivo no existe, pero este nombre de archivo se está supervisando (nunca ha existido o puede que se haya suprimido)
Última modificación	Indicación de fecha y hora de la última modificación, tomada del sistema de archivos en el tiempo del muestreo
Fecha de última modificación	Fecha de la última modificación
Día de la semana de la última modificación	Día de la semana de la última modificación
Año de última modificación	Año de la última modificación

Grupo	Solo en UNIX. Si el tipo de elemento es un archivo, el propietario del grupo.

Entidad Configuración de host

Atributo	Descripción
ID de etiqueta de estado de auditoría	Identificador numérico exclusivo para el elemento de configuración
Nombre de host	Nombre de host o dirección IP del servidor de bases de datos
Tipo de SO	Sistema operativo: Unix o Windows
Tipo de BD	Tipo de base de datos (Oracle, MS-SQL, DB2, Sybase, Informix, etc.) o N/D si el cambio ocurre en una instancia de sistema operativo
Nombre de instancia	Nombre de la instancia del conjunto de plantillas
Tipo	Tipo de elemento supervisado que ha cambiado. Script de SO o Script SQL: Cambio desencadenado por el script de SO contenido en la definición de plantilla de elemento supervisado. Variable de entorno: una variable de entorno (sólo Unix) Variable de registro: una variable de registro (sólo Windows) Archivo: un archivo específico. No hay ninguna entidad de configuración de host para un patrón de archivo definido en el conjunto de plantillas utilizado por la instancia. En su lugar, hay una entidad de configuración de host distinta para cada archivo que coincide con el patrón.
Elemento supervisado	Nombre del elemento modificado, de la Descripción (si se ha especificado), de lo contrario, es un nombre predeterminado que depende del tipo (un nombre de archivo, por ejemplo).

Entidad Datos guardados

Atributo	Descripción
ID de datos guardados	Identificador numérico único para el elemento de datos guardados
Datos guardados	Datos reales guardados
Indicación de fecha y hora	Indicación de fecha y hora del momento en que se registró la entidad de datos guardados en la base de datos del servidor
Identificador de cambio	Identifica la entidad de cambios supervisados para esta entidad de datos guardados

Informes predeterminados de dominio de cambios de CAS

Informe predeterminado	Descripción
Detalles de cambios de CAS	Para cada elemento supervisado, lista los cambios por propietario. Este informe lista los cambios realizados en el archivo, por ejemplo el propietario o los permisos de acceso. No lista los cambios realizados en el contenido del archivo.
Datos guardados de CAS	Lista los datos de cada cambio detectado de los elementos supervisados con el recuadro opcional Conservar datos seleccionado. El informe lista los cambios realizados en el contenido del archivo, pero no en las propiedades.

Detalles de cambios de CAS

Entidad	Atributo	Operador	Valor predeterminado
Configuración de host	DB_Type	Like	%
Configuración de host	Host_Name	Like	%
Configuración de host	Instance_Name	Like	%
Configuración de host	Monitored_Item	Like	%
Configuración de host	OS_Type	Like	%
Configuración de host	Tipo	Like	%

Informes detallados

Informe	Descripción
Detalles del registro	Muestra los datos guardados incluidos en la columna Recuento de datos guardados

Datos guardados de CAS

Entidad	Atributo	Operador	Valor predeterminado
Configuración de host	Host_Name	Like	%
Configuración de host	Monitored_Item	Like	%
Cambios supervisados	Saved_Data_Id	Like	%

Informes detallados

Informe	Descripción
Ver diferencia	Muestra la diferencia entre los datos seleccionados y la versión anterior

Tema principal: CAS (Configuration Auditing System)

Estado de CAS (Configuration Auditing System)

Abra el Estado de CAS haciendo clic en Gestionar > Supervisión de cambios > Estado de CAS

Para cada servidor de base de datos en el que se ha instalado y ejecutado CAS, y en el que el sistema Guardium está configurado como servidor activo del host de Guardium, este panel muestra el estado de CAS y el estado de cada instancia de CAS configurada para el servidor de base de datos.

Si tiene problemas para distinguir los colores de las luces del indicador de estado, coloque el ratón sobre las luces de estado y un recuadro le mostrará el estado actual.

Componente	Descripción
Luz de indicador de estado del sistema CAS	La luz que se encuentra en este panel indica si CAS se está ejecutando de manera activa en el sistema Guardium. Rojo: CAS no se está ejecutando en el sistema Guardium. Verde: CAS está activo en el sistema Guardium.
Luces de indicador de estado del agente de CAS	Estas luces de estado indican si el agente de CAS está conectado al sistema Guardium. Identifican cada agente de CAS referenciando la dirección IP que aparece antes de la fila de las luces de indicador de estado **Rojo**: El host y/o el agente de CAS están fuera de línea o no se puede acceder a ellos. **Verde**: El host y el agente de CAS están en línea. **Amarillo:** El sistema Guardium es secundario para el host de CAS.
Restablecer	Restablece el agente de CAS en este sistema supervisado. Esto detiene y reinicia el agente de CAS en el servidor de base de datos. Nota: También restablecerá los archivos de punto de comprobación, lo que permite iniciar y escanear los archivos desde cero.
Suprimir (X)	Elimina el sistema supervisado CAS y suprime los datos del sistema Guardium asociados con el cliente CAS. Este botón se inhabilita si el agente de CAS se está ejecutando en el sistema. Debe detener el agente de CAS para poder suprimirlo. Consulte Detención e inicio de sesión del agente de CAS para obtener más información.
Luz roja/amarilla/verde	Cada conjunto de luces indica el estado de una instancia de CAS en el sistema supervisado. Si el estado del sistema supervisado poseedor es de color rojo (lo que indica que el agente de CAS está fuera de línea), ignore este conjunto de luces de estado. **Rojo**: La instancia está inhabilitada. **Verde**: La instancia está habilitada y en línea y la configuración se sincroniza con la configuración del sistema Guardium. **Amarillo**: Se habilita la instancia, pero la configuración de la misma en el sistema Guardium no coincide con la configuración de la instancia del sistema supervisado (se ha actualizado en el sistema Guardium, pero la actualización no se ha aplicado en el sistema supervisado).
Renovar	Pulse Renovar para volver a comprobar el estado de todos los servidores de la lista. Este botón no se detiene ni reinicia CAS en el servidor de base de datos; comprueba la conexión entre CAS en el sistema Guardium y CAS en cada servidor de base de datos.

Nota: Se requiere la entrada TAP_IP en el archivo guard_tap.ini. Si falta TAP_IP, CAS no se iniciará y se registrará un mensaje de error en el archivo de registro del cliente CAS.

Detención e inicio del agente de CAS

Existen varias situaciones en las que es posible que deba detener o iniciar el agente de CAS en un sistema supervisado.
Nota: Si desea detener y reiniciar el agente de CAS, puede hacerlo pulsando Gestionar > Supervisión de cambios > Estado de CAS.

Detención de CAS en un host UNIX

1. Edite el archivo /etc/inittab.
2. Busque la línea respawn de CAS:

```
cas:2345:respawn:/usr/local/guardium/guard_stap/cas/bin/run_wrapper.sh /usr/local/guardium/guard_stap/cas/bin
```

3. Comente la línea insertando # en la posición del primer carácter.
4. Guarde el archivo.
5. Especifique el mandato siguiente: init -q
6. Especifique el mandato siguiente: ps -er | grep cas
7. Anote el PID de cada uno de los procesos de la lista.
8. Emita el siguiente mandato para cada uno de los procesos de la lista: kill -9 <pid>
9. En el panel Estado de CAS (Configuration Auditing System) del portal de administrador de Guardium, la luz de estado para el host de CAS debería estar en rojo y el botón Eliminar habilitado. Esto le permite eliminar datos del host de CAS en la base de datos interna del sistema Guardium.

Inicio de CAS en un host de Unix

Utilice este procedimiento para iniciar el agente CAS solo cuando se haya detenido editando el archivo /etc/inittab, tal y como se ha descrito anteriormente.

1. Edite el archivo /etc/inittab.
2. Busque la línea:

```
#cas:2345:respawn:/usr/local/guardium/guard_stap/cas/bin/run_wrapper.sh /usr/local/guardium/guard_stap/cas/bin
```

3. Elimine el comentario de la línea, en nuestro ejemplo (paso 2), eliminando # de la primera posición de carácter. En función del sistema operativo, el carácter de comentario puede ser otro.
4. Guarde el archivo.
5. Especifique el mandato siguiente para reiniciar el agente de CAS: init -q

Inicio y detención de CAS en un host de Windows

En Windows, CAS se ejecuta como un servicio de sistema.

1. En el panel Servicios, resalte el elemento del cliente CAS.
2. Seleccione Iniciar o Detener en el menú Acción.

Tema principal: CAS (Configuration Auditing System)

Configuración del sistema Guardium

Puede configurar varios aspectos del sistema Guardium para satisfacer sus objetivos empresariales de forma más efectiva y eficaz.

- Configuración del sistema
  La mayor parte de la información del panel Configuración del sistema se establece utilizando la CLI en el momento de la instalación.
- Configuración del motor de inspección
  Un motor de inspección supervisa el tráfico entre un conjunto de uno o más servidores y un conjunto de uno o más clientes utilizando un protocolo de base de datos específico (por ejemplo, Oracle o Sybase).
- Configuración de portal
  Puede mantener el servidor web del dispositivo de Guardium en su puerto predeterminado (8443) o restablecer el portal. Le recomendamos encarecidamente que utilice el puerto predeterminado.
- Generar nuevo diseño
- Configurar la autenticación
  De forma predeterminada, Guardium autentica los inicios de sesión de usuario de Guardium, independientemente de cualquier otra aplicación.
- Perfil global
  El panel Perfil global define valores predeterminados aplicables a todos los usuarios.
- Configuración del alertador
  No se enviarán mensajes de correo electrónico, excepciones SNMP o mensajes relacionados con alertas hasta que el alertador esté configurado y activado.
- Detección de anomalías
  El proceso Detección de anomalías ejecuta cada intervalo de sondeo para crear y guardar, pero no enviar, notificaciones de alerta de correlación basadas en una consulta de alerta.
- Inferencia de sesiones
  Inferencia de sesiones comprueba si hay sesiones abiertas que han estado inactivas durante un periodo de tiempo especificado, y las marca como cerradas.
- Creación de alias IP-Nombre de host
  La función Creación de alias IP-Nombre de host accede al servidor DNS (Domain Name System) para definir alias de nombre de host para direcciones IP de cliente y servidor.
- Copia de seguridad del sistema
  Utilice la función Copia de seguridad del sistema para definir una operación de copia de seguridad que se pueda ejecutar a petición o de una forma planificada. Utilice la función Copia de seguridad de parche para crear los valores de perfil de copia de seguridad.
- Configuración de la copia de seguridad de parche
  Utilice esta característica para almacenar la información de perfiles de copia de seguridad.
- Configurar permiso para la conexión de socket
  Este tema se aplica a las clases de alertas personalizadas.

Configuración del sistema

La mayor parte de la información del panel Configuración del sistema se establece utilizando la CLI en el momento de la instalación.

Para obtener instrucciones sobre cómo configurar el sistema, o para modificar cualquier otro valor de Configuración del sistema, consulte Modificar la configuración del sistema.

Debe haber una licencia válida para utilizar diversas funciones en el dispositivo. Cuando se especifica una licencia después de que se inicia el sistema, se requiere reiniciar la interfaz gráfica de usuario.

Acerca del secreto compartido del sistema

El administrador de Guardium define el secreto compartido del sistema en la Configuración del sistema. El secreto compartido del sistema se utiliza para dos fines generales:

- Para cifrar los archivos que se exportan del dispositivo mediante actividades de archivado/exportación
- Para establecer comunicaciones seguras entre gestores centrales y unidades gestionadas

Si utiliza gestión central y/o agregación, debe establecer el secreto compartido del sistema para todos los sistemas en el mismo valor.

El valor del secreto compartido del sistema es nulo en el momento de la instalación. En función de las prácticas de seguridad de una empresa, es posible que sea necesario cambiar el secreto compartido del sistema de forma periódica. Cada dispositivo mantiene un archivo de claves secretas compartido, que contiene un registro histórico de todos los secretos compartidos definidos en dicho dispositivo. El mismo sistema, por lo tanto, no tendrá ningún problema posteriormente para descifrar información que se haya cifrado en ese sistema.

Cuando se exporta o se archiva información desde un sistema, y se importa o se restaura en otro, este último debe tener acceso al secreto compartido utilizado por el primero. Para estos casos, hay mandatos de CLI que se pueden utilizar para exportar los secretos compartidos del sistema desde un sistema Guardium e importarlos en otro.

Consulte los mandatos siguientes en el apéndice de la CLI:

- aggregator backup keys file

- aggregator restore keys file

Modificación de la configuración del sistema

1. Pulse Configuración > Herramientas y vistas > Sistema para abrir la Configuración del sistema.
2. Realice los cambios.
3. Pulse Aplicar para guardar la configuración actualizada del sistema.

Nota: Los cambios aplicados no entran en vigor hasta que se reinicia el sistema Guardium. Después de aplicar los cambios de configuración, pulse Reiniciar para detener y reiniciar el sistema.

Tabla 1. Consulta del panel Configuración del sistema

Campo o control	Descripción
Identificador global exclusivo	Este valor se utiliza para la clasificación y agregación de datos. El valor predeterminado es un valor exclusivo que se deriva de la dirección MAC de la máquina. No cambie este valor después de que el sistema empiece las operaciones de supervisión.
Secreto compartido de sistema	Cualquier valor que especifique aquí no se visualizará. Todos los caracteres que especifique se enmascararán. El secreto compartido del sistema se utiliza para las operaciones de archivado/restauración, así como para las operaciones de gestión central y agregación. Cuando se utiliza, su valor debe ser el mismo para todas las unidades que se comunicarán. Este valor es nulo en el momento de la instalación y se puede cambiar con el tiempo. Se utiliza el secreto compartido del sistema: • Cuando se están estableciendo conexiones seguras entre un Gestor central y una unidad gestionada. • Cuando una unidad agregada firma y cifra datos para la exportación al agregador. • Cuando una unidad firma y cifra datos para el archivado. • Cuando un agregador importa datos de una unidad agregada. • Cuando una unidad restaura datos archivados. En función de las prácticas de seguridad de la empresa, es posible que tenga que cambiar el secreto compartido del sistema de vez en cuando. Puesto que el secreto compartido puede cambiar, cada sistema mantiene un archivo de claves secretas compartido, que contiene un registro histórico de todos los secretos compartidos definidos en ese sistema. Esto permite que un archivo exportado (o archivado) de un sistema con un secreto compartido anterior sea importado (o restaurado) por un sistema en el que ese mismo secreto compartido haya sido sustituido por uno más nuevo. **Precaución**: Cuando lo utiliza, asegúrese de guardar el valor de secreto compartido en una ubicación segura. Si pierde el valor, no podrá acceder a los datos archivados.
Reescribir secreto	Cuando especifique o cambie el secreto compartido del sistema, vuelva a escribir el nuevo valor una segunda vez. Cualquier valor que especifique aquí no se visualizará. Todos los caracteres que especifique se mostrarán como un asterisco.
Clave de licencia	La clave de licencia se inserta en la configuración durante la instalación. No modifique este campo a menos que así se lo indique el soporte técnico. Es posible que deba pegar una nueva clave de producto aquí si se están añadiendo componentes opcionales. Si instala una nueva clave de producto en la unidad de gestión central, cuando pulse Aplicar, recibirá un mensaje de aviso que indicará: `Aviso: Si cambia la licencia en una unidad de gestión central es necesario renovar la información en todas las unidades gestionadas.` Después de pulsar Aceptar para cerrar la ventana de mensaje, debe pulsar Aplicar por segunda vez para instalar la nueva clave de producto. Sabrá que la licencia nueva se ha instalado cuando reciba el mensaje: `Los datos se han guardado de forma satisfactoria.` Si instala una nueva clave de producto en una unidad de gestión central, es posible que reciba un aviso que indique que la licencia aplicada al Gestor central se debe renovar en la unidad gestionada. Esto requiere una renovación realizada desde el Gestor central y se realiza pulsando el icono de renovación desde el Gestor central para cada uno de los recopiladores listados. La licencia autoriza al usuario a acceder a los productos y a las características correspondientes. La licencia se puede añadir o sobrescribir. La licencia activa se almacena en LICENSE_KEY en ADMINCONSOLE_PARAMETER Tipos de producto DAM; FAM; VA Edición de los tipos de producto: Express; Standard; Advanced
Número de orígenes de datos	Si se aplica una licencia limitada, se muestra el número máximo de orígenes de datos permitidos por licencia de origen de datos.
Escaneos de medición restantes	Si se aplica una licencia limitada, se muestra el número de exploraciones de asesoramiento de vulnerabilidades permitidas (medición de origen de datos) por licencia de medición. Cada vez que se desencadena un asesoramiento dex vulnerabilidades, el contador de exploración disminuye en uno.
Licencia válida hasta	Si se aplica una licencia limitada, se muestra una fecha fija en la que la licencia se inhabilitará.
Número de licencias	Este valor indica el número de licencias restantes.
Nota: Configure los valores de dirección de red, interfaz de gestión secundaria y direccionamiento utilizando la CLI	Estos valores no se pueden configurar mediante la interfaz gráfica de usuario y aparecen en gris en la interfaz de usuario de la Configuración del sistema.
Nombre de host de sistema	El nombre de host que se puede resolver para el sistema Guardium. Este nombre debe coincidir con el nombre de host DNS para la dirección IP del sistema principal.
Dominio	El nombre del dominio DNS en el que reside el sistema Guardium.
Dirección IP de sistema	La dirección IP primaria que utilizan los usuarios y los agentes de CAS o S-TAP para conectarse al sistema Guardium. Se asigna a la interfaz de red denominada ETH0.
Máscara de subred	La máscara de subred para la dirección IP del sistema primaria.

Campo o control	Descripción
Dirección de hardware (MAC)	La dirección MAC de la interfaz de red primaria.

Dirección IP de sistema (secundaria)	Opcional: También se puede configurar un puerto para trabajar con la interfaz primaria con el fin de proporcionar un equipo de IP de sustitución por anomalía de alta disponibilidad.
	
	Como alternativa, se puede configurar un puerto del dispositivo como una interfaz de gestión secundaria con una dirección IP, máscara de red y pasarela distintas de las primarias.
	
	Estas dos opciones se excluyen mutuamente.
	
	Existen dos tipos de conexiones de gestión secundarias, distintas y mutuamente excluyentes, que se controlan ambas mediante opciones del mismo mandato de CLI:
	
	Acoplamiento o creación de equipo
	Convierte eth0 y otra tarjeta de interfaz de red (NIC) especificada en un par acoplado con sustitución por anomalía en espera. Para implementar esta opción, utilice el mandato de CLI store network interface high-availability on <nic>, donde nic es una NIC disponible.
	Interfaz secundaria
	Permite que la interfaz gráfica de usuario y la CLI sean accesibles desde otra NIC en el sistema Guardium. Para implementar esta opción, utilice el mandato de la CLI store network interface secondary on <nic> <ip> <mask> <gateway> para especificar la NIC secundaria, su dirección IP y máscara de red y, opcionalmente, una pasarela.
	
	Los sistemas físicos y de VM tienen AMBOS las mismas prestaciones, según el número de NIC instaladas en el sistema Guardium o VM.
	
	Para visualizar las interfaces de red instaladas en la unidad, utilice el mandato de CLI **show network interface inventory**. Por ejemplo:
	
	`show network interface inventory`
	`Current network card configuration:`
	`Device  | Mac Address  |Member of`
	`----------`
	`eth0  |  00:50:56:3b:c3:73  |`
	`eth1  |  00:50:56:8a:0d:fa  |`
	`eth2  |  00:50:56:8a:0d:fb  |`
	`eth3  |  00:50:56:8a:00:c1  |`
	
	Nota: "Member of" mostrará qué NIC están en un par de acoplamiento, si existe un acoplamiento.
	
	Para localizar los conectores eth en el dispositivo, utilice el mandato de CLI **show network interface port**, que parpadeará la luz naranja en ese puerto, 20 veces. Por ejemplo:
	
	guard14.xyz.com> sho net int port 3
	
	La luz naranja en el puerto eth5 ahora parpadeará 20 veces.
	
	Nota: La dirección IP secundaria y su puerto asociado NO están relacionados con la característica de alta disponibilidad, que proporciona soporte de sustitución por anomalía mediante equipo de IP para la conexión primaria. Para obtener más información sobre la opción de alta disponibilidad, consulte los mandatos de CLI **store network interface** en el Apéndice de CLI.

Máscara de subred (secundaria)	Opcional. Máscara de subred para la dirección IP del sistema secundaria.
Ruta predeterminada/ Ruta secundaria	Dirección IP del direccionador predeterminado para el sistema./ Dirección IP del direccionador secundario
Resolvedor primario Resolvedor secundario Resolvedor terciario	Se requiere la dirección IP del resolvedor primario (DNS). El secundario y el terciario son opcionales.
Probar conexión	Pulse Probar conexión para probar la conexión con el servidor DNS (Sistema de nombres de dominio) correspondiente. Esto sólo comprueba que haya acceso al puerto 53 (DNS) en el host especificado. No verifica que se trate de un servidor DNS operativo. Recibirá un cuadro de mensaje que indicará si el servidor DNS ha respondido.
Detener	Pulse Detener para cerrar el sistema.
Reiniciar	Pulse Reiniciar para detener y volver a iniciar el sistema. Se le solicitará que confirme la acción.
Aplicar	Pulse Aplicar para guardar los cambios. Los cambios se aplicarán la próxima vez que se reinicie el sistema.

Tema principal: Configuración del sistema Guardium

Configuración del motor de inspección

Un motor de inspección supervisa el tráfico entre un conjunto de uno o más servidores y un conjunto de uno o más clientes utilizando un protocolo de base de datos específico (por ejemplo, Oracle o Sybase).

El motor de inspección extrae SQL de los paquetes de red; compila los árboles de análisis que identifican sentencias, solicitudes, mandatos, objetos y campos; y registra información detallada acerca de ese tráfico en una base de datos interna.

Puede configurar e iniciar o detener varios motores de inspección en el dispositivo de Guardium.

Los motores de inspección no se pueden definir ni ejecutar en una unidad de Gestor central. Sin embargo, puede iniciar y detener los motores de inspección en las unidades gestionadas desde el panel de control del Gestor central.

Los motores de inspección también se definen en los S-TAP. Si los S-TAP informan a este dispositivo de Guardium, asegúrese de que el dispositivo no supervise el mismo tráfico que el S-TAP. Si esto sucede, el motor de análisis recibirá paquetes duplicados, no podrá reconstruir los mensajes e ignorará ese tráfico.

Selección de direcciones IP

Cada motor de supervisión supervisa el tráfico entre una o varias direcciones IP de cliente y servidor. En una definición de motor de inspección, éstas se definen utilizando una dirección IP y una máscara. Puede considerar una dirección IP como una única ubicación y una máscara como un mecanismo de comodín que le permite definir un rango de direcciones IP.

Las direcciones IP tienen el formato: n.n.n.n, donde cada n es un número de ocho bits (denominado un octeto) en el rango de 0 a 255.

Por ejemplo, una dirección IP para el PC podría ser: 192.168.1.3. Esta dirección se utiliza en los ejemplos. Puesto que estos son números binarios, el último octeto (3) se puede representar como: 00000011.

La máscara se especifica en el mismo formato que la dirección IP: n.n.n.n. Un cero en cualquier posición de bits de la máscara sirve como un comodín. Por lo tanto, la máscara 255.255.255.240 combinada con la dirección IP 192.168.1.3 coincide con todos los valores de 0-15 en el último octeto, ya que el valor 240 en binario es 11110000. Pero sólo coincide con los valores 192.168.1 en los tres primeros octetos, ya que 255 es todo 1 en binario (en otras palabras, no se aplican comodines para los tres primeros octetos).

La especificación de máscaras binarias puede ser un poco confusa. Sin embargo, en aras de la comodidad, las direcciones IP suelen estar agrupadas de forma jerárquica, con todas las direcciones de una categoría (por ejemplo, los sistemas de sobremesa) agrupadas en uno de los dos últimos octetos. Por lo tanto, en la práctica, los números que se ven con más frecuencia en las máscaras son 255 (sin comodín) o 0 (todos).

Por lo tanto, una máscara 255.255.255.255 (que no tiene bits 0) identifica sólo la dirección especificada por la dirección IP (en este ejemplo, 192.168.1.3).

Como alternativa, la máscara 255.255.255.0, combinada con la misma dirección IP, coincide con todas las direcciones IP que empiezan por 192.168.1.

Selección de todas las direcciones

La dirección IP 0.0.0.0, que a veces se utiliza para indicar todas las direcciones IP, no está permitida en Guardium. Para seleccionar todas las direcciones IP cuando se utiliza una combinación de dirección IP/máscara, utilice cualquier dirección IP distinta de cero seguida de una máscara que contenga todos los ceros (por ejemplo: 1.1.1.1/0.0.0.0). Sin embargo, 0.0.0.0/0.0.0.0 es una combinación válida.

Configurar valores aplicables a todos los motores de inspección

1. Pulse Gestionar > Supervisión de actividad > Motores de inspección para abrir la Configuración de motor de inspección.
2. Consulte la tabla y realice los cambios que desee.
3. Pulse Aplicar para guardar la configuración actualizada del sistema cuando haya terminado de realizar cambios.
4. Si lo desea, añada comentarios a la configuración de motor de inspección.
5. Pulse Reiniciar motores de inspección.

Nota: Los cambios realizados no tienen efecto hasta que se reinician los motores de inspección. Después de aplicar los cambios en la configuración de motor de inspección, pulse el botón Reiniciar para detener y reiniciar el sistema (utilizando los nuevos valores de configuración).
Nota: Para el soporte HTTP existen limitaciones de la configuración de motor de inspección. Los siguientes valores del motor de inspección no están soportados para HTTP: Valor de captura predeterminado; Predeterminado marcar confirmación automática; Creación de secuencias de registro; Serie SQL de excepción de registro; Registrar registros afectados; Calcular tiempo de respuesta promedio; Inspeccionar datos devueltos; Grabar sesiones vacías.

Tabla 1. Valores aplicables a todos los motores de inspección

Control	Descripción
Valor de captura predeterminado	El valor predeterminado es falso. Lo utiliza la función de reproducción para distinguir entre transacciones y valores de captura, lo que significa que si tiene una sentencia preparada, los valores asignados se capturarán y reproducirán. Si desea reproducir las sentencias preparadas capturadas como sentencias preparadas, el recuadro de selección debe estar marcado para los datos capturados.
Predeterminado marcar confirmación automática	El valor predeterminado es verdadero. Debido a varios modelos de confirmación automática para distintas bases de datos, este valor lo utiliza la función de reproducción para marcar explícitamente las transacciones y la confirmación automática después de cada mandato. Nota: Si el recuadro de selección está marcado, las confirmaciones y retrotracciones se ignorarán. Entre las bases de datos soportadas actualmente se incluyen DB2, Informix y Oracle.
Creación de secuencias de registro	Si está marcado, se crea un registro de la sentencia SQL inmediatamente anterior, así como de la sentencia SQL actual, siempre y cuando la construcción anterior tenga lugar en un periodo de tiempo lo suficientemente corto.
Serie SQL de excepción de registro	Si está marcado, cuando se registran las excepciones, se registra toda la sentencia SQL.

Control	Descripción
Registrar registros afectados	Registros afectados: Conjunto de resultados del número de registros que se ven afectados por cada ejecución de sentencias SQL. Si está marcado, se registra el número de registros afectados para cada sentencia SQL (cuando sea aplicable). El valor predeterminado para los registros afectados es FALSE (0). Nota: Cuando se utiliza JDBC, se debe marcar para registrar correctamente el tráfico de variables de enlace de Oracle Nota: La opción Registros afectados es una operación de sniffer para procesar paquetes de respuesta adicionales y posponer el registro de los datos afectados, lo que incrementa el tamaño del almacenamiento intermedio y potencialmente podría tener un efecto adverso en el rendimiento global de sniffer. Las respuestas realmente grandes causan un impacto considerable. Para evitar la gran sobrecarga asociada con esta operación, Guardium utiliza un conjunto de umbrales predeterminados que permite que sniffer decida omitir la operación de proceso cuando se sobrepasa. Nota: Normalmente, Registros afectados está establecido correctamente cuando el usuario activa Registrar registros afectados mediante Motores de inspección > Registrar registros afectados. Sin embargo, si se utiliza MS-SQL mediante procedimiento almacenado se establecerá Registros afectados como -1. Consulte Mandatos de CLI de configuración y control store max_results_set_size, store max_result_set_packet_size y store max_tds_response_packets, para establecer niveles de granularidad. Ejemplo de valores de conjunto de resultados: • Caso 1, valor de registros afectados, número positivo: Esto representa el tamaño correcto del conjunto de resultados. • Caso 2, valor de registros afectados, -2: Esto significa que el número de registros ha superado el límite configurable (se puede ajustar a través de los mandatos de CLI). • Caso 3, valor de registros afectados, -1: Muestra los casos no soportados por Guardium de configuraciones de paquetes. • Caso 4, valor de registros afectados, -2: Si el conjunto de resultados se envía por modalidad continua. • Caso 5, valor de registros afectados, -2: El resultado intermedio durante el recuento de registros para poner al día al usuario sobre el valor actual, acaba con un número positivo de registros totales. Nota: La característica Registros afectados no está soportada en DB2 cuando se utiliza la modalidad continua para enviar los resultados.
Calcular tiempo de respuesta promedio	Cuando está marcado, para cada construcción de SQL registrada, se calculará el tiempo de respuesta promedio.
Inspeccionar datos devueltos	Marque este control para inspeccionar los datos devueltos por las solicitudes de SQL, así como para actualizar los recuentos de entrada y salida. Si se van a utilizar reglas en la política de seguridad, este recuadro de selección debe estar marcado.
Grabar sesiones vacías	Cuando está marcado, se registrarán las sesiones que no contienen sentencias SQL. Cuando no esté marcado, estas sesiones se ignorarán.
Analizar XML	El motor de inspección normalmente no analizará el tráfico XML. Marque este recuadro de selección para analizar el tráfico XML.
Granularidad de registro	El número de minutos (1, 2, 5, 10, 15, 30 o 60) en una unidad de registro. Si se solicita en un informe, Guardium resume los datos de solicitud en esta granularidad. Por ejemplo, si la granularidad de registro es 60, se ha producido una cierta solicitud n veces en una hora determinada. Si el recuadro de selección no está marcado, no se registra cuándo exactamente durante la hora se ha producido el mandato. Sin embargo, si una solicitud desencadena una regla de una política, una alerta en tiempo real puede indicar la hora exacta. Cuando se definen reglas de excepción para una política, esas reglas también se pueden aplicar a la unidad de registro. Por ejemplo, es posible que desee omitir 5 anomalías de inicio de sesión por hora, pero enviar una alerta cuando se produzca el sexto error de inicio de sesión.
Máximo de aciertos por datos devueltos	Cuando se inspeccionen los datos devueltos, indique el número de hits (infracciones de reglas de política) que se registrarán.
Lista de puertos ignorados	Una lista de los puertos que deben ignorarse. Añada valores a esta lista si sabe que los servidores de bases de datos están procesando protocolos que no son de base de datos y desea que Guardium no desperdicie ciclos analizando tráfico que no es de base de datos. Por ejemplo, si sabe que el host en el que reside la base de datos también ejecuta un servidor HTTP en el puerto 80, puede añadir 80 a la lista de puertos ignorados, asegurándose de que Guardium no procesará estas corrientes de datos. Separe varios valores con comas, y utilice un guión para especificar un rango de puertos inclusivo. Por ejemplo: 101,105,110-223
Almacenamiento intermedio libre: n %	Visualización solamente. **n** es el porcentaje de espacio libre de almacenamiento intermedio disponible para el proceso del motor de inspección. Este valor se actualiza cada vez que se renueva la ventana. Hay un proceso de un solo motor de inspección que controla todos los motores de inspección. Es el almacenamiento intermedio utilizado por dicho proceso.
Reiniciar motores de inspección	Pulse Reiniciar motores de inspección para detener y reiniciar todos los motores de inspección.
Añadir comentarios	Pulse Comentario para añadir comentarios a la configuración de motor de inspección.
Aplicar	Pulse Aplicar para guardar la configuración. Nota: Los cambios globales realizados (y guardados utilizando Aplicar) no entran en vigor hasta que se reinician los motores de inspección. Sin embargo, los atributos individuales del motor de inspección, como la exclusión, el orden de secuencia, etc., entran en vigor inmediatamente.

Crear un motor de inspección

1. Pulse Gestionar > Supervisión de actividad > Motores de inspecciónpara abrir Motores de inspección.
2. Pulse Añadir motor de inspección para expandir el panel.
3. Especifique un nombre en el recuadro Nombre. Debe ser exclusivo en el dispositivo. Recomendamos que sólo utilice letras y números en el nombre, ya que el uso de cualquier carácter especial impide trabajar con este motor de inspección a través de la CLI.
4. En el recuadro Protocolo, seleccione el protocolo que se va a supervisar (Aster, Cassandra, CouchDB, DB2, DB2 Exit, exclude IE, FTP, GreenPlumDB, Hadoop, HIVE, HTTP, HUE, IBM ISERIES, IMPALA, Informix, iNFORMIX Exit, KERBEROS, Maria,DB, MongoDB, MS SQL, Mysql, Named Pipes, Netezza, Oracle, PostgreSQL, SAP

Hana, Sybase, Teradata, WebHDFS or Windows File Share) o la palabra clave exclude IE. Seleccione exclude IE si desea que se omita todo el tráfico entre los servidores y clientes especificados.
Nota: Exclude IE sólo funciona en los puertos, independientemente de la IP. Especifique un rango de puertos que se debe omitir. Para excluir una IP específica para este puerto, se puede utilizar la IP de cliente de BD de exclusión en el motor de inspección creado. Si es necesario no seleccionar paquetes en un rango de puertos determinado, defina un motor de inspección aparte del tipo Exclude IE (IGNORE). Los únicos valores que se deben definir en ese motor son PORT_RANGE_START y PORT_RANGE_END. Este tipo de exclusión puede ser necesario, por ejemplo, cuando se define un motor de inspección de Oracle todo incluido con el rango de puertos 1024-65535, pero se deben excluir determinados puertos. Cuando utilice Oracle para Windows, amplíe el rango de puertos a 1000-65535.
Nota: Cuando se envíe tráfico IPC desde la base de datos de GreenPlum, se registrará en el sistema Guardium como tráfico de PostgresSQL. Cuando se envíe tráfico TCP desde la base de datos de GreenPlum, se conectará como base de datos de GreenPlum con el motor de inspección. Para el tráfico TCP, Guardium determina la base de datos de acuerdo con el puerto (puerto 5432 para GreenPlum). Para el tráfico IPC, Guardium utiliza conducto con nombre y, para la base de datos de GreenPlum, el sistema Guardium utiliza PostgresSQL como el nombre de la base de datos. Cuando ambas bases de datos, PostgresSQL y Greenplum, están en el mismo sistema, su tráfico IPC se registrará en DB_PROTOCOL, según el primer IE de base de datos PostgresSQL/Greenplum establecido en el archivo guard_tap.ini.

5. En los recuadros IP/Máscara de cliente de BD, especifique una lista de clientes (un host de cliente desde el que se ha iniciado la conexión de base de datos) que se deben supervisar (o excluir si se marca el recuadro Excluir IP de cliente de BD). Los clientes se identifican por las direcciones IP y las máscaras de subred. En la visión general encontrará instrucciones detalladas sobre cómo utilizar estos campos.

   Pulse el signo más para añadir una dirección IP y una máscara de subred adicionales. Pulse el signo menos para eliminar la última dirección IP y máscara de subred.

6. En los recuadros IP/Máscara de servidor de BD, especifique una lista de servidores de bases de datos (donde se encuentra una base de datos) que se deben supervisar. Los servidores se identifican por las direcciones IP y las máscaras de subred. En la visión general encontrará instrucciones detalladas sobre cómo utilizar estos campos.

   Pulse el signo más para añadir una dirección IP y una máscara de subred adicionales. Pulse el signo menos para eliminar la última dirección IP y máscara de subred.

7. En el recuadro Puerto, especifique un único puerto o un rango de puertos sobre los que se supervisará el tráfico entre los servidores de bases de datos y los clientes especificados. Con frecuencia sería un único puerto.

   Aviso: No especifique un amplio rango de puertos sólo para estar seguro de que ha incluido el correcto! Puede hacer que el motor de inspección se atasque intentando analizar el tráfico en los puertos que no tiene tráfico de base de datos o tráfico que no es de interés para su entorno.

8. Marque el recuadro Activo al iniciar si este motor de inspección se debe iniciar automáticamente durante el arranque.
9. Marque el recuadro Excluir IP de cliente de BD si desea que el motor de inspección supervise el tráfico de todos los clientes excepto los listados en la lista IP/Máscara de cliente de DB. Asegúrese de que comprende la diferencia entre este control y la selección Ignorar protocolo. Esta incluye todo el tráfico excepto de las direcciones desde IP. Para omitir un conjunto específico de clientes sin incluir todos los demás clientes, defina un motor de inspección distinto para estos clientes y utilice Ignorar protocolo.
10. Pulse Añadir para guardar la definición.
11. Opcionalmente, vuelva a colocar el motor de inspección en la lista de motores de inspección. Los mecanismos de filtrado definidos en los motores de inspección se ejecutan por orden. Si es necesario, vuelva a posicionar la nueva configuración de motor de inspección, o cualquier otra configuración existente, utilizando los botones Arriba y/o Abajo en el borde de la definición.
12. Opcionalmente, pulse Iniciar para iniciar el motor de inspección que acaba de configurar. Una vez que se haya iniciado el motor, el botón Iniciar se sustituirá por un botón Detener.
13. Nota: Si proporciona un valor para TAP_IDENTIFIER y el valor contiene espacios, Guardium reemplazará automáticamente los espacios con guiones. Por ejemplo, el valor "Descripción de ejemplo" se convertirá en "Descripción-de-ejemplo".

Iniciar o detener un motor de inspección

Pulse Gestionar > Supervisión de actividad > Motores de inspecciónpara abrir los Motores de inspección. Para iniciar un motor de inspección, pulse Iniciar. Para detener un motor de inspección, pulse Detener.

Eliminar un motor de inspección

Si ya no está utilizando un motor de inspección, le sugerimos que elimine la definición, para que no se reinicie de forma accidental.

1. Pulse Gestionar > Supervisión de actividad > Motores de inspección para abrir el Motor de inspección.
2. Si el motor de inspección que se va a eliminar no se ha detenido, pulse Detener.
3. Para eliminar un motor de inspección, pulse Suprimir.

Tema principal: Configuración del sistema Guardium

Configuración de portal

Puede mantener el servidor web del dispositivo de Guardium en su puerto predeterminado (8443) o restablecer el portal. Le recomendamos encarecidamente que utilice el puerto predeterminado.

1. Pulse Configuración > Herramientas y vistas > Portalpara abrir el Portal.
2. Si no está marcado, marque el recuadro de selección Activar al iniciar (nunca debería estar inhabilitado).
3. Establezca el Puerto HTTPS en un valor entero entre 1025 y 65535.
4. Pulse Aplicar para guardar el valor. (El portal de seguridad de Guardium no empezará a escuchar en este puerto hasta que se reinicie.) O bien pulse Revertir para restaurar el valor almacenado por la última operación Aplicar.
5. Si ha realizado y guardado cambios, pulse Reiniciar para reiniciar el servidor web de Guardium. Ahora puede conectarse a la unidad en el puerto que acaba de asignar.
   Nota: Para volver a conectarse a la unidad después de que se haya reiniciado con el nuevo número de puerto, debe cambiar el URL utilizado para abrir la página de inicio de sesión de Guardium en el navegador.

Se utiliza la configuración del portal de Guardium para definir cómo se autentican las contraseñas de usuario al iniciar sesión en el dispositivo de Guardium. Hay tres opciones.

Estas opciones son Local (valor predeterminado de Guardium), RADIUS o LDAP.

La pantalla Configuración del portal en Configuración > Herramientas y vistas > Portal se utiliza para lo siguiente:

1. Para definir la mejor manera de autenticar una contraseña de usuario.
2. Para reiniciar la interfaz gráfica de usuario para restablecer el tipo de autenticación.

La conexión Local funcionará cuando se defina una contraseña para un usuario determinado desde un inicio de sesión. El inicio de sesión se define utilizando el rol accessmgr. De forma predeterminada, inicie sesión en la cuenta **accessmgr**, que tiene el rol accessmgr. Este rol proporciona a un usuario la capacidad de añadir o subir cuentas de usuario y de crear contraseñas.

Cuando defina el nombre de usuario y la contraseña utilizando el tipo de rol accessmgr, la contraseña definida por usuario se utilizará al iniciar sesión en el dispositivo de Guardium.

La conexión RADIUS permite la autenticación de inicio de sesión mediante un servidor radius. El servidor Radius/RSA se puede definir utilizando una contraseña y un número de señal SecurID. La contraseña numérica de señal SecurID se muestra mediante una señal de hardware.

El servidor Radius/RSA se define en un servidor Windows. La señal SecurID RSA de seguridad también se define y almacena en el servidor Radius y no es necesario descargarla para que funcione el portal Radius.

También se puede definir una conexión de servidor Radius utilizando una plataforma UNIX. Radius también se define como FreeRadius. La cuenta de usuario y las contraseñas se definen en los servidores Radius y no es necesario descargarlas. Para utilizar FreeRadius, el cliente (el servidor de Guardium), el nombre de usuario y las contraseñas se definen en los servidores UNIX de FreeRadius y se utilizan cuando se define la conexión del portal Radius.

El portal predeterminado se establece en Local.

La conexión LDAP funcionará cuando se defina la contraseña y se almacene en un servidor LDAP determinado. Para que un usuario pueda utilizar el portal LDAP e iniciar sesión, primero debe importarse un nombre de cuenta de usuario desde **el servidor LDAP**. Utilice la función Importación LDAP de usuario disponible desde la cuenta accessmgr para definir la ubicación de LDAP y, a continuación, importe los usuarios de LDAP. No es necesario subir la contraseña.

Tema principal: Configuración del sistema Guardium

Generar nuevo diseño

Generar un nuevo diseño para un rol basado en un diseño de usuario

El administrador o el gestor de acceso de Guardium puede generar, a través de CLI, un diseño predeterminado para un rol. A continuación, cualquier usuario nuevo que tenga asignado ese rol tendrá dicho diseño después de iniciar sesión por primera vez.

Nota: El usuario de administración pueden definir estructuras .psml predeterminadas para rol y usuario, mediante la interfaz gráfica de usuario. Consulte Editor de portlets para obtener más información.

Utilice el mandato de CLI generate-role-layout para generar un nuevo diseño para un rol existente, basado en el diseño para el usuario especificado. Una vez que se ha definido el nuevo diseño de rol, todos los usuarios a los que se haya asignado ese rol antes de iniciar sesión por primera vez recibirán el diseño para ese rol.

generate-role-layout

Sintaxis generate-role-layout <usuario> <rol>

Nota: usuario (nombre de inicio de sesión) y rol no son sensibles a mayúsculas y minúsculas.

Parámetros

Si alguno de los dos parámetros siguientes contiene espacios (John Doe es el usuario o Gestores DBA es el rol), sustituya los espacios por caracteres de subrayado.

Por ejemplo:

generate-role-layout John_Doe Gestores_DBA

usuario: Nombre del usuario cuyo diseño se va a utilizar como modelo para el diseño de rol. Si el usuario no existe, recibirá el mensaje de error siguiente: `No existe el usuario '<usuario>'.`

rol: Rol al que se conectará el nuevo diseño.

Tema principal: Configuración del sistema Guardium

Configurar la autenticación

De forma predeterminada, Guardium autentica los inicios de sesión de usuario de Guardium, independientemente de cualquier otra aplicación.

Para la cuenta de usuario de administración de Guardium, el inicio de sesión lo autentica sólo Guardium. Para todas las demás cuentas de usuario de Guardium, la autenticación se puede configurar para utilizar RADIUS o LDAP. En estos últimos casos, se requiere información de configuración adicional para la conexión al servidor de autenticación.
Nota: Se da soporte al software de cliente FreeRadius.

Cuando se utiliza un método de autenticación alternativo, todos los usuarios de Guardium deben aún estar definidos como usuarios en el dispositivo Guardium. La otra aplicación lo único que hace es la autenticación.

Mientras que el usuario accessmgr gestiona las cuentas de usuario y los roles, el método de autenticación lo gestiona el usuario admin. Esta es la práctica recomendada estándar de separación de responsabilidades.

Para configurar la autenticación, consulte el tema siguiente.

Configurar la autenticación de Guardium

1. Pulse Configuración > Herramientas y vistas > Portal para abrir la Configuración de autenticación.

2. Seleccione el botón Guardium en el panel Configuración de autenticación.
3. Pulse Aplicar.

Configurar autenticación de RADIUS

1. Pulse Configuración > Herramientas y vistas > Portal para abrir la Configuración de autenticación.
2. Seleccione el botón RADIUS en el panel Configuración de autenticación. Aparecerán campos adicionales en el panel.
3. En el recuadro Servidor primario, especifique el nombre de host o dirección IP del servidor RADIUS primario.
4. Opcionalmente, especifique el nombre de host o la dirección IP de los servidores RADIUS secundario y terciario.
5. Especifique el puerto UDP (1812 o 1645) que utiliza RADIUS.
6. Especifique el secreto compartido de servidor RADIUS, dos veces.
7. Especifique los segundos de tiempo de espera (el valor predeterminado es 120).
8. Seleccione el tipo de autenticación:
   - PAP - protocolo de autenticación de contraseña
   - CHAP - protocolo de autenticación de reto-reconocimiento
   - MS-CHAPv2 - Microsoft versión 2 del protocolo de autenticación reto-reconocimiento
9. Pulse opcionalmente Probar para verificar la configuración. Se le informará de los resultados de la prueba. La configuración también se probará cada vez que pulse el botón Aplicar para guardar cambios.
10. Pulse Aplicar.Guardium intentará autenticar un usuario de prueba y le informará de los resultados.

Configurar autenticación LDAP

1. Pulse Configuración > Herramientas y vistas > Portal para abrir la Configuración de autenticación.
2. Seleccione el botón LDAP en Configuración de autenticación.
3. En el recuadro Servidor, especifique el nombre de host o la dirección IP del servidor LDAP.
4. Especifique el número de Puerto (el valor predeterminado es 636 para LDAP sobre SSL).
5. Especifique el tipo de usuario RDN (tipo de nombre distinguido relativo), que de forma predeterminada es UID.
   Nota:

   Este atributo identifica a un usuario para la autenticación LDAP. El gestor de acceso debe ser consciente de qué atributo se utiliza aquí, ya que el gestor de acceso realiza la operación Importar usuarios LDAP. Pulse en este enlace de ayuda, Importar usuarios LDAP, para obtener información adicional sobre la importación de usuarios LDAP.

   Si el usuario utiliza SamAccountName como valor de RDN, el usuario debe utilizar =search o =[nombre de dominio] en el nombre completo.

   Ejemplos: SamAccountName=search, SamAccountName=dom

6. Especifique el DN base de usuario (nombre distinguido).
7. Marque o desmarque el recuadro Utilizar SSL, según sea adecuado para su servidor LDAP.
8. Opcional. Para inspeccionar uno o más certificados de confianza, pulse Certificados de confianza y siga las instrucciones de ese panel.
9. Opcional. Para añadir un certificado de confianza, pulse Añadir certificados de confianza y siga las instrucciones de ese panel.
10. Opcional. Pulse Probar para verificar la configuración. Se le informará de los resultados de la prueba. También se probará la configuración cada vez que pulse Aplicar para guardar los cambios.
11. Pulse Aplicar.Guardium intentará autenticar un usuario de prueba y le informará de los resultados.

Tema principal: Configuración del sistema Guardium

Perfil global

El panel Perfil global define valores predeterminados aplicables a todos los usuarios.

Alterar temporalmente el valor de alias predeterminado

De forma predeterminada, para cualquier informe nuevo, o para cualquier informe que esté contenido en un diseño predeterminado, no se utilizan alias.

Un alias proporciona un sinónimo que se sustituye por un valor almacenado de un tipo de atributo específico. Se utiliza normalmente para mostrar un nombre descriptivo o fácil de usar para un valor de datos. Por ejemplo, es posible que el servidor financiero se haya definido como un alias para la dirección IP 192.168.2.18.

Si desea ver los alias de forma predeterminada, puede cambiar el valor de alias predeterminados para todos los informes, como se indica a continuación:

- Pulse Configuración > Herramientas y vistas > Perfil global para abrir el Perfil global.
- Marque el recuadro de selección Utilizar alias en informes a menos que se especifique lo contrario.
- Pulse Aplicar.

Personalizar el pie de página de PDF

Los archivos PDF creados por diversos componentes de Guardium (tareas de auditoría, por ejemplo) tienen un pie de página estándar. Para personalizar esa cabecera:

1. Pulse Configuración > Herramientas y vistas > Perfil global para abrir el Perfil global.
2. En el campo Texto de pie de página de PDF, especifique el texto que se imprimirá en el pie de cada página.
   Nota: El texto de pie de página de PDF no se distribuye desde el Gestor central/agregador a las unidades gestionadas.
3. Pulse Aplicar.

Editar la plantilla de mensaje de alerta

Para personalizar la plantilla de mensaje utilizada para generar alertas:

1. Pulse Configuración > Herramientas y vistas > Perfil global para abrir el Perfil global.
2. En el recuadro de texto Plantilla de mensaje, edite el texto de la plantilla de alerta.

   Puede marcar el recuadro de texto Sin ajuste para ver dónde se parte la línea que aparece en el mensaje.

3. Pulse Aplicar cuando haya terminado.
4. Los cambios no se aplican hasta que se reinician los motores de inspección. Para hacer esto ahora, pulse Gestionar > Supervisión de actividad > Motores de inspección para abrir los Motores de inspección. Pulse Reiniciar motores de inspección.

Tabla 1. Variables de plantilla de mensaje de alerta

Variable	Descripción
%%addBaselineConstruct	Para añadir a línea base Atención: El Creador de línea base y su funcionalidad está en desuso desde Guardium V10.1.4.
%%AppUserName	Nombre de usuario de la aplicación
%%AuthorizationCode	Código de autorización
%%category	Categoría de la definición de regla
%%classification	Clasificación de la definición de regla
%%clientHostname	Nombre de host del cliente
%%clientIP	Dirección IP del cliente
%%clientPort	Número de puerto del cliente
%%DBName	Nombre de la base de datos
%%DBProtocol	Protocolo de la base de datos
%%DBProtocolVersion	Versión del protocolo de la base de datos
%%DBUser	Nombre de usuario de la base de datos
%%lastError	Descripción de último error; disponible sólo cuando una solicitud de error de SQL que desencadena una regla de excepción contiene un campo de descripción de último error
%%netProtocol	Protocolo de red, para K-TAP en Oracle, puede mostrarse como IPC o BEQ
%%OSUser	Información de la sesión. (OS_USER en GDM_ACCESS)
%%receiptTime	Indicación de fecha y hora que representa la hora a la que se produjo la alerta
%%receiptTimeMills	Cifra que representa la hora a la que se produjo la alerta, en milisegundos, desde la fecha fija del 1 de enero de 1900
%%requestType	Tipo de solicitud
%%ruleDescription	Descripción de la regla de la definición de regla de política
%%ruleID	Número de regla de la definición de regla
%%serverHostname	Nombre de host del servidor
%%serverIP	Dirección IP del servidor
%%serverPort	Número de puerto del servidor
%%serverType	Tipo de servidor de base de datos
%%serviceName	Nombre del servicio
%%DBName	Nombre de la base de datos
%%sessionStart	Hora de inicio de sesión (hora de inicio de sesión)
%%sessionStartMills	Cifra que presenta el inicio de la sesión donde se ha producido la alerta, en milisegundos, desde la fecha fija del 1 de enero de 1900
%%severity	Gravedad de la definición de regla
%%SourceProgram	Nombre del programa fuente
%%SQLNoValue	Serie SQL con valores enmascarados. El valor de SQL se sustituirá con ? en syslog.
%%SQLString	Serie SQL (si hay alguna)
%%SQLTimestamp	Hora en el paquete/solicitud (TIMESTAMP en GDM_CONSTRUCT_TEXT)
%%Subject[ ]	Si esta variable se utiliza en la plantilla de mensaje, todo lo que aparece entre [ ] (por ejemplo, nombre de archivo, remitente de correo electrónico, descripción) será la línea de asunto del correo electrónico enviado al usuario.
%%violationID	Cifra que representa el POLICY_VIOLATION_LOG_ID de esta alerta en GDM_POLICY_VIOLATION_LOG (es igual que el ID de registro de infracción en el informe Infracciones de política/Gestión de incidentes)

Plantilla con nombre

Las plantillas de mensaje se utilizan para generar alertas.

La característica define varias plantillas de mensaje y facilita el uso de distintas plantillas en distintas reglas. En el pasado, sólo había una única plantilla de mensaje disponible para todas las reglas, todos los tipos de destinatario, etc.

Para añadir, modificar y suprimir las plantillas de mensaje con nombre, pulse Editar. Al crear una nueva plantilla con nombre, el valor de inicio de la serie es una copia de lo que esté actualmente en la plantilla de mensaje del Perfil global. "Alerta de en tiempo real" es el único nivel de gravedad permitido.

Se han creado plantillas de mensajes predefinidas para las soluciones de SIEM, ArcSight, EnVision y QRadar. El sistema Guardium se entrega precargado con dos plantillas certificadas (acordadas) para su integración con estas dos soluciones SIEM.

El creador de plantillas con nombre puede seleccionar entre dos tipos de plantilla: Alertas en tiempo real e Informe de proceso de auditoría.

Utilice el Informe de proceso de auditoría para auditar tareas de proceso.

Pulse Editar plantillas con nombre. Elija un SIEM y a continuación pulse Modificar. Seleccione Alertas en tiempo real o Informe de proceso de auditoría.

Después de editarlas, las distintas plantillas de mensaje se pueden seleccionar en el menú Creador de políticas. Consulte Políticas.

La adición de la plantilla de QRadar le permite enviar alertas en tiempo real o informes de proceso de auditoría a QRadar utilizando el formato LEEF (este es el formato de QRadar).

Siga los pasos para enviar alertas en tiempo real o resultados de proceso de auditoría a la SIEM de QRadar.

Alerta en tiempo real, Guardium a QRadar

1. Cree una alerta en tiempo real.
2. Escriba en syslog
3. Seleccione el tipo de plantilla (alerta en tiempo real)
4. Reenvíe a Q1 Labs QRadar SIEM (mediante plantilla de mensaje predefinida/correlación LEEF): elija plantilla con nombre de QRadar del Perfil Global
5. En la CLI, ejecute el mandato de CLI "store remotelog" para reenviar los mensajes de syslog a QRadar.

Informe de proceso de auditoría, Guardium a QRadar

Pulse Reforzar > Asesoramiento de vulnerabilidades > Creador de procesos de auditoría para abrir el Creador de procesos de auditoría.

1. Cree un informe de proceso de auditoría (creador de proceso de auditoría)
2. Escriba en syslog
3. Seleccione el tipo de plantilla (informe de proceso de auditoría)
4. Reenvíe a Q1 Labs QRadar SIEM (mediante plantilla de mensaje predefinido/correlación LEEF): elija plantilla con nombre de QRadar del Perfil Global
5. En la CLI, ejecute el mandato de CLI "store remotelog" para reenviar los mensajes de syslog a QRadar.

Por ejemplo, la siguiente es la plantilla LEEF predeterminada para el informe Bases de datos descubiertas:

```
LEEF:0|IBM|Guardium|9.0|Databases Discovered|Time Probed=${1}|Server IP=${2}|Server Host Name=${3}|DB
Type=${4}|Port=${5}|Port Type=${6}
```

Estas son las columnas del informe que se correlacionan con la plantilla:

```
Hora del análisis      IP de servidor    Nombre de host de servidor    Tipo de BD    Puerto    Tipo de puerto
```

1. Seleccione Exportar a archivo CSV y Escribir en Syslog.
2. Seleccione la plantilla con nombre, Bases de datos descubiertas LEEF
3. Configure el syslog remoto mediante el mandato store remotelog. Por ejemplo:

   ```
   store remotelog add user.info 9.70.145.68 udp
   ```

   Esto enviará todos los registros del proceso de auditoría a la dirección IP proporcionada.

Codificación del remitente

Para codificar los mensajes salientes (correo electrónico y excepciones SNMP) en un esquema de codificación que no sea UTF8, utilice el mandato de CLI, store sender_encoding.

Filtre las plantillas de un solo tipo

Hay un mecanismo de filtro para seleccionar todas las alertas en tiempo real o informe de proceso de auditoría. Marque o desmarque cada selección.

Plantilla de mensaje de Envision 2

GUARDIUM_ALERT:
rule-id=%%ruleID^^category=%%category^^classification=%%classification^^severity=%%severity^^session-start-time=%%sessionStart^^client-hostname=%%clientHostname^^client-ip=%%clientIP^^server-type=%%serverType^^server-ip=%%serverIP^^src-program=%%SourceProgram^^os-user=%%OSUser^^db-user=%%DBUser^^app-user=%%AppUserName^^service-name=%%serviceName^^req-type=%%requestType^^rule-desc=%%ruleDescription^^sql=%%SQLNoValue

Plantilla predeterminada de umbral

Como en las alertas en tiempo real, puede seleccionar una plantilla para el mensaje que se envía cuando se alcanza el umbral. La plantilla utiliza una lista predefinida de variables que se sustituyen por el valor apropiado para la alerta específica.

Esas variables son:

%%alertName - nombre de la alerta

%%description - descripción de la alerta

%%alertQueryValue - valor de consulta que ha causado la alerta

%%alertThreshold - umbral de la alerta

%%alertQueryFromDate - inicio del periodo de consulta

%%alertQueryToDate - fin del periodo de consulta

%%alertBaseQueryValue - valor de consulta base de la alerta

%%classification - clasificación de la alerta

%%category - categoría de alerta

%%severity - gravedad de la alerta

%%recommendation - acción recomendada de la alerta

%%Subject[] - asunto del mensaje

La plantilla predeterminada para alertas de umbral es la siguiente (se puede clonar y editar):

%%Subject[Guardium Alert. Gravedad: (%%severity), Nombre de alerta: %%alertName]

Nombre de alerta: %%alertName. Descripción de alerta: %%description.

Valor actual: %%alertQueryValue

Valor de consulta base: %%alertBaseQueryValue

Umbral: %%alertThreshold

Periodo consulta: %%alertQueryFromDate - %%alertQueryToDate

Clasificación de alerta: %%classification

Categoría: %%category

Gravedad: %%severity

Acción recomendada: %%recommendation

Personalizar alertas en tiempo real y correo electrónico

Controle el aspecto del asunto de correo electrónico del prefijo con el nombre de dispositivo de Guardium.
Controle el aspecto del asunto de correo electrónico en el cuerpo del correo electrónico.
Añada el parámetro de denominación de plantilla %%applianceHostName para que los usuarios de Guardium puedan añadir el nombre de host de dispositivo para dar nombre a plantillas (cualquier posición, asunto o cuerpo).
Para hacer esto, utilice dos campos de la tabla ADMINCONSOLE_PARAMETERS:
APPEND_APPLIANCENAME_SUBJECT
APPEND_SUBJECT_IN_BODY
Utilice los siguientes mandatos de CLI para controlar el contenido de estos campos:
show alerter email append_name_subject
store alerter email append_name_subject
mostrar o almacenar el distintivo para añadir el nombre de dispositivo en el asunto del correo electrónico
show alerter email append_subject_body
store alerter email append_subject_body mostrar o almacenar el distintivo para añadir el asunto de correo electrónico al inicio del cuerpo del correo electrónico
Cada vez que el valor en la CLI cambia, se aplica inmediatamente en los correos electrónicos salientes.

Separador de CSV

Para definir un separador para que se utilice en el proceso de auditoría:

1. Pulse Configuración > Herramientas y vistas > Perfil global para abrir el Perfil global.
2. Seleccione coma, punto y coma, tabulador o bien defina su propio separador en el recuadro Otros para definir el separador de CSV que se utilizará.
3. Pulse Aplicar.

Añadir otro contenido HTML a la ventana de Guardium

Para añadir otro contenido HTML a la ventana de Guardium:

1. Pulse Configuración > Herramientas y vistas > Perfil global para abrir el Perfil global.
2. En los recuadros de texto HTML - izquierda y HTML - derecha, especifique el HTML para el texto o cualquier otro elemento que desee incluir en la ventana.
3. Opcionalmente, pulse el botón de vista previa para verificar que el HTML se visualiza de la forma esperada.
4. Pulse Aplicar.

Añadir o inhabilitar un mensaje de inicio de sesión

Para añadir un mensaje para que se muestre en un recuadro de mensaje, cada vez que un usuario inicie sesión:

1. Pulse Configuración > Herramientas y vistas > Perfil global para abrir el Perfil global.
2. En el recuadro de texto Mensaje de inicio de sesión, especifique el texto que desee que se muestre cada vez que el usuario inicia sesión.
3. Marque el recuadro Mostrar mensaje de inicio de sesión para habilitar la visualización del mensaje de inicio de sesión (o desmarque el recuadro para inhabilitar su visualización).
4. Pulse Aplicar.

Habilitar o inhabilitar inicios de sesión simultáneos del mismo usuario

De forma predeterminada, el mismo usuario de Guardium puede iniciar sesión en un dispositivo desde varias direcciones IP. Puede inhabilitar los inicios de sesión simultáneos de un mismo usuario. Cuando está inhabilitado, se permitirá a cada usuario de Guardium iniciar sesión desde solo una única dirección IP cada vez. Si un usuario cierra su navegador sin cerrar la sesión, la conexión excederá el tiempo de espera debido a la inactividad, por lo que la cuenta de usuario no estará bloqueada mucho tiempo.

Para modificar este valor:

1. Pulse Configuración > Herramientas y vistas > Perfil global para abrir el Perfil global.
2. Localice el campo ID de sesión simultáneo desde IP diferentes.
3. Pulse Habilitar o Inhabilitar, según el estado actual, para cambiar el valor.
   Nota: Cuando la característica está inhabilitada, aparece un botón Desbloquear junto al botón Habilitar. Puede pulsar Desbloquear para permitir que un segundo usuario inicie sesión con esta cuenta de usuario, desde una dirección IP distinta. Se proporciona con fines de soporte.

Habilitar seguridad a nivel de datos en nivel de datos observados

Esta característica presupone que usuarios específicos de Guardium son responsables de determinadas bases de datos. Por lo tanto, existe un mecanismo que filtrará los resultados, en todo el sistema, de modo que cada usuario podrá ver la información sólo de las bases de datos de las que el usuario es responsable.

Restricción: La seguridad a nivel de datos y el panel de control de investigación no se pueden habilitar simultáneamente.

Para modificar este valor:

1. Pulse Configuración > Herramientas y vistas > Perfil global para abrir el Perfil global.
2. Pulse el botón Habilitar o Inhabilitar para la opción de filtrado de seguridad a nivel de datos
   Nota: El rol datasec-exempt se activa cuando la seguridad a nivel de datos está habilitada y el rol datasec-exempt se ha asignado a un usuario.
3. Las opciones adicionales incluyen:
   - Show-all: Permite que la persona con la sesión iniciada visualice todas las filas del resultado, independientemente de a quién pertenezcan esas filas. Cuando se utiliza con el rol Datasec-exempt, permite una alteración temporal del filtrado de seguridad a nivel de datos.
   - Incluir registros indirectos: Permite que la persona con la sesión iniciada visualice las filas pertenecientes al usuario con la sesión iniciada, pero también todas las filas pertenecientes a los usuarios que están por debajo del usuario con la sesión iniciada en la jerarquía.

Nota: Si la seguridad de datos a nivel de datos observados está habilitada, se permite el escalado del proceso de auditoría sólo a los usuarios en un nivel superior en la jerarquía de usuarios.

Filtrado predeterminado

Valor predeterminado de visor en línea y para distribución de resultados de proceso de auditoría.

Show-all. El valor predeterminado está inhabilitado.

Escalar el resultado a todos los usuarios

Escalar el resultado a todos los usuarios: Una marca de selección en este recuadro escala los resultados de proceso de auditoría (y versiones en PDF) a todos los usuarios, incluso si la seguridad a nivel de datos en el nivel de datos observados está habilitada. El valor predeterminado está habilitado. Si el recuadro de selección está inhabilitado (no hay ninguna marca de selección en el recuadro), se permite el escalado de proceso de auditoría sólo a los usuarios en un nivel superior en la jerarquía de usuarios y a usuarios con el rol datasec-exempt. Si el recuadro de selección está inhabilitado, y no hay ninguna jerarquía de usuarios, no se permite ningún escalado.

Tamaño máximo de tabla de base de datos personalizada

Establezca el tamaño de la tabla de base de datos personalizada (en MB). El valor predeterminado es 4000 MB.

En este punto en el menú Perfil global hay un botón para ver el Uso actual. Pulse el botón Uso actual para que se muestren los valores de INNODB, MYISAM y Total.

Nota: El límite de tamaño personalizado se prueba antes de la importación de los datos. La importación puede superar el límite máximo de tamaño. Cuando se supere el límite, no se podrá realizar la siguiente importación.

Archivos SCP y FTP mediante distintos puertos

Cambie los puertos que puede utilizar para enviar archivos a través de SCP y FTP.

Perfil global: se puede modificar la copia de seguridad de parche y la exportación. El puerto predeterminado para ssh/scp/sftp es 22. El puerto predeterminado para FTP es 21.
Nota: Si ve un cero (0) como puerto en la interfaz gráfica de usuario de Guardium, esto indica que se está utilizando el puerto predeterminado y que no es necesario cambiarlo.

Añadir un logotipo a la ventana de Guardium

Para añadir un gráfico del logotipo de la empresa a la ventana de Guardium, o para añadir cualquier otro contenido HTML a la ventana de Guardium:

1. Pulse Configuración > Herramientas y vistas > Perfil global para abrir el Perfil global.
2. En Subir imagen de logotipo, si desea incluir una imagen de logotipo en la ventana del portal, especifique un nombre de archivo de imagen o pulse Examinar para seleccionar un archivo para subir al dispositivo de Guardium, y a continuación pulse Subir.
3. Renueve la ventana del navegador. Aparece el nuevo logotipo.

Nota: El nombre del archivo de logotipo subido no puede contener comillas simples, comillas dobles, el signo menor que ni el signo mayor que.

Cifrar Must Gather

Se ha añadido Cifrar Must Gather al Perfil global. El valor predeterminado está deseleccionado (No cifrar). Si está desmarcado, la salida de Must Gather está sólo comprimida y no cifrada. Cuando el recuadro está seleccionado, en el futuro toda la salida Must Gather siempre se cifrará. También se puede establecer el cifrado mediante el mandato de CLI store encrypt_must_gather on, o bien desactivarlo mediante store encrypt_must_gather off.

Comprobar actualizaciones de Guardium

Si se añade una marca de comprobación, se mostrarán todos los parches relevantes de Guardium ad hoc, GPU/CFP/paquetes, parches de Sniffer y parches de seguridad que estén disponibles para que el cliente los descargue. Una vez que se ha instalado un paquete, este aparecerá en la lista.

Tiempo de espera excedido de la conexión del origen de datos

Establezca el tiempo de espera de la conexión del origen de datos en segundos. El valor predeterminado es 60 segundos.

El mandato GrdAPI correspondiente para actualizar este valor es: grdapi update_datasource_connection_timeout timeoutInSecond=80

Tema principal: Configuración del sistema Guardium

Configuración del alertador

No se enviarán mensajes de correo electrónico, excepciones SNMP o mensajes relacionados con alertas hasta que el alertador esté configurado y activado.

Otros componentes crean y ponen en cola mensajes para el alertador. El alertador comprueba y envía mensajes según el intervalo de sondeo que tiene configurado.

Para configurar, habilitar o inhabilitar alertas de correlación individuales, consulte Alertas de correlación. Para que se generen alertas de correlación y alertas de dispositivo, debe estar iniciada también la detección de anomalías. Para que se generen alertas en tiempo real, debe estar instalada una política de seguridad.

Los mensajes Mail/SNMP/SYSLOG se envían según su prioridad.

Activar automáticamente el alertador al iniciar

1. Pulse Configuración > Herramientas y vistas > Alertador para abrir el Alertador o pulse Proteger > Detección de intrusión en base de datos > Alertador para abrir el Alertador.
2. Seleccione el recuadro Activo al iniciar. Cada vez que se reinicie el dispositivo, el alertador se activará automáticamente.
3. Pulse Aplicar.
4. Si el alertador no se está ejecutando y desea iniciarlo, pulse Reiniciar.

Establecer la frecuencia con la que el alertador comprueba si hay mensajes y envía mensajes

1. Pulse Configuración > Herramientas y vistas > Alertador para abrir el Alertador o pulse Proteger > Detección de intrusión en base de datos > Alertador para abrir el Alertador.
2. Especifique el intervalo de sondeo, en segundos.
3. Pulse Aplicar.

Configurar el alertador para enviar mensajes SMTP (correo electrónico)

1. Pulse Configuración > Herramientas y vistas > Alertador para abrir el Alertador o pulse Proteger > Detección de intrusión en base de datos > Alertador para abrir el Alertador.
   Nota: Todos los demás elementos de este tema se encuentran en la sección SMTP del panel Alertador.
2. Especifique la dirección IP de la pasarela SMTP, en el recuadro Dirección IP.
3. Especifique el número de puerto SMTP (es casi siempre 25) en el recuadro Puerto.
4. Opcional: pulse el enlace de hipertexto Probar conexión para verificar la dirección y el puerto SMTP. Esto sólo prueba que haya acceso al puerto y host especificados. No verifica que se trate de un servidor SMTP operativo. Se visualiza un recuadro de diálogo que le informe del éxito o error de la operación.
   Nota: Si este servidor SMTP utiliza autenticación, debe proporcionar un nombre de usuario y contraseña válidos para ese servidor de correo en los dos campos siguientes. De lo contrario, estos campos estarán en blanco.
5. Especifique un nombre de usuario válido para el servidor de correo en el recuadro Nombre de usuario si el servidor SMTP utiliza autenticación.
6. Especifique la contraseña del usuario en el recuadro Contraseña si el servidor SMTP utiliza autenticación. Vuelva a especificarla en el recuadro Vuelva a especificar la contraseña.
7. En el recuadro Dirección de correo electrónico de devolución, especifique la dirección de devolución del correo electrónico enviado por el sistema. Esta dirección normalmente es una cuenta administrativa que se comprueba a menudo.
8. Seleccione Autoriz. en el recuadro Método de autenticación si su servidor SMTP utiliza autenticación. De lo contrario, seleccione Ninguno. Cuando se selecciona Autoriz., debe especificar el nombre de usuario y la contraseña que se deben utilizar para la autenticación.
9. Pulse Aplicar para guardar la configuración.
   Nota: el alertador no empezará a utilizar la nueva configuración hasta que se reinicie.
10. Pulse Reiniciar para reiniciar el alertador con la nueva configuración.

Configure el alertador para enviar excepciones SNMP

1. Pulse Configuración > Herramientas y vistas > Alertador para abrir el Alertador o pulse Proteger > Detección de intrusión en base de datos > Alertador para abrir el Alertador.
   Nota: Todos los demás elementos de este tema se encuentran en la sección SMTP del panel Alertador.
2. En el recuadro Dirección IP, especifique la dirección IP a la que se enviará la excepción SNMP.
3. Opcional: pulse el enlace de hipertexto Probar conexión para verificar la dirección y el puerto SNMP (162). Esto sólo prueba que haya acceso al puerto y host especificados. No verifica que se trate de un servidor SNMP operativo. Se visualiza un recuadro de diálogo que le informe del éxito o error de la operación.
4. En el recuadro ”Trap” Community, especifique el nombre de comunidad de la excepción. Vuelva a especificar la comunidad en el recuadro Volver a escribir comunidad.
5. Pulse Aplicar para guardar la configuración.
   Nota: el alertador no empezará a utilizar la nueva configuración hasta que se reinicie.
6. Pulse Reiniciar para reiniciar el alertador con la nueva configuración.

Tema principal: Configuración del sistema Guardium

Detección de anomalías

El proceso Detección de anomalías ejecuta cada intervalo de sondeo para crear y guardar, pero no enviar, notificaciones de alerta de correlación basadas en una consulta de alerta.

Esta notificación se ejecuta según la planificación definida para cada alerta. Consulte Configuración del alertador para obtener más información acerca del envío de notificaciones.

El proceso Detección de anomalías utiliza los resultados de una consulta de alerta de correlación, que examina un periodo de tiempo especificado y el umbral de la alerta de correlación, para determinar si se cumple una condición (por ejemplo, un número excesivo de inicios de sesión fallidos). Consulte Alertas de correlación para obtener más información.

En un entorno del Gestor central, se puede utilizar el panel Detección de anomalías de cada sistema Guardium para desactivar las alertas de correlación que no son apropiadas para ese sistema Guardium en particular. En Gestión central, todas las alertas de correlación se definen en el Gestor central, independientemente de en qué sistema Guardium se hayan creado o actualizado. Estas alertas de correlación son las mismas para todos los sistemas Guardium y, cuando se activan, se activan de forma predeterminada en todos los sistemas Guardium.

Nota: El componente Alertador debe estar configurado e iniciado para enviar un mensaje de alerta guardado a SYSLOG, correo electrónico o una excepción SNMP.

Nota: Detección de anomalías no tiene ningún rol en la producción de alertas en tiempo real, que generan las políticas de seguridad.

Activar automáticamente la detección de anomalías al iniciar

1. Pulse Configuración > Herramientas y vistas > Detección de anomalías para abrir Detección de anomalías.
2. Seleccione el recuadro Activo al iniciar. Cada vez que se reinicia el sistema Guardium, la detección de anomalías se activa automáticamente.
3. Pulse Aplicar.

Establecer la frecuencia con la que la detección de anomalías comprueba si hay problemas con el dispositivo

1. Pulse Configuración > Herramientas y vistas > Detección de anomalías para abrir Detección de anomalías.
2. Especifique el intervalo de sondeo en minutos.
3. Pulse Aplicar.

Habilitar o inhabilitar alertas activas

Para inhabilitar una alerta globalmente en un entorno de Gestor central, es más fácil desmarcar el recuadro de selección Activo en el panel Modificar alerta.

Para habilitar o inhabilitar una alerta en un único sistema Guardium en un entorno de Gestión central, siga estos pasos:

1. Inicie sesión en la interfaz de usuario del sistema Guardium en el que desea inhabilitar una o más alertas.
2. Pulse Configuración > Herramientas y vistas > Detección de anomalías para abrir Detección de anomalías.
3. Para inhabilitar una alerta, selecciónela en el recuadro Alertas activas y pulse Inhabilitar.
4. Para habilitar una alerta, selecciónela en el recuadro Alertas inhabilitadas localmente y pulse Habilitar.

Detener o reiniciar la detección de anomalías

1. Pulse Configuración > Herramientas y vistas > Detección de anomalías para abrir Detección de anomalías.
2. Pulse Detener para detener la detección de anomalías, o pulse Reiniciar para reiniciarla.

Tema principal: Configuración del sistema Guardium

Inferencia de sesiones

Inferencia de sesiones comprueba si hay sesiones abiertas que han estado inactivas durante un periodo de tiempo especificado, y las marca como cerradas.

Para configurar las opciones de Inferencia de sesiones:

1. Pulse Configuración > Inferencia de sesiones para abrir Inferencia de sesiones.
2. Marque el recuadro Activo al iniciar para iniciar Inferencia de sesiones cuando se inicie el sistema Guardium.
3. En el recuadro Intervalo de sondeo, especifique la frecuencia (en minutos) con la que Inferencia de sesiones comprueba si hay sesiones abiertas. El valor predeterminado es 120 (minutos).
4. En el recuadro Periodo máximo de inactividad, especifique el número de minutos de inactividad tras los cuales una sesión se marcará como cerrada. El valor predeterminado es 720 (minutos).
5. Pulse Aplicar para almacenar los valores en la base de datos de configuración. Inferencia de sesiones no empezará a utilizar una nueva configuración hasta que se reinicie.
6. Pulse Reiniciar para reiniciar Inferencia de sesiones con la nueva configuración.

Para detener Inferencia de sesiones, abra el panel Inferencia de sesiones y pulse Detener.

Tema principal: Configuración del sistema Guardium

Creación de alias IP-Nombre de host

La función Creación de alias IP-Nombre de host accede al servidor DNS (Domain Name System) para definir alias de nombre de host para direcciones IP de cliente y servidor.

Hay dos conjuntos de direcciones IP: uno para clientes y otro para servidores. Cuando Creación de alias IP-Nombre de host está habilitado, los nombres de alias reemplazarán las direcciones IP en Guardium donde corresponda.

1. Pulse Proteger > Detección de intrusión en base de datos > Creación de alias IP-Nombre de host para abrir Creación de alias IP-Nombre de host.
2. Marque el recuadro de selección Generar alias de nombre de host para IP de cliente y servidor (si están disponibles) para habilitar la creación de alias de nombre de host.

   Ahora se puede acceder a un segundo recuadro de selección. El nombre de este recuadro de selección es Actualizar alias de nombre de host existentes si se redescubren.

3. Marque el recuadro de selección para actualizar un alias definido anteriormente que no coincide con el nombre de host DNS actual (lo que normalmente indica que el nombre de host de esta dirección IP ha cambiado). Puede que no desee hacer esto si ha asignado manualmente algunos alias. Por ejemplo, suponga que el nombre de host DNS de una dirección IP determinada es dbserver204.guardium.com, pero ese servidor se conoce comúnmente como el servidor QA Sybase. Si se ha definido manualmente el servidor QA Sybase como un alias de esa dirección IP, y el recuadro de selección Actualizar alias de nombre de host existentes si se redescubren está marcado, el nombre de host DNS sobrescribirá ese alias.
4. Pulse Aplicar para guardar la configuración de creación de alias IP-Nombre de host.
5. Realice una de las opciones siguientes:
   - Pulse Ejecutar una vez ahora para generar los alias inmediatamente.
   - Pulse Definir planificación para definir una planificación para ejecutar esta tarea. Consulte Planificación para obtener más información.

Para ver los alias definidos, consulte Alias.

Tema principal: Configuración del sistema Guardium

Copia de seguridad del sistema

Utilice la función Copia de seguridad del sistema para definir una operación de copia de seguridad que se pueda ejecutar a petición o de una forma planificada. Utilice la función Copia de seguridad de parche para crear los valores de perfil de copia de seguridad.

Copia de seguridad del sistema

Las copias de seguridad del sistema se utilizan para realizar copias de seguridad de todos los datos y valores de configuración necesarios y utilizarlos para restaurar un servidor en caso de que el hardware resulte dañado.

Toda la información y los datos de configuración se graban en un único archivo cifrado y se envían al destino especificado, utilizando el método de transferencia configurado para las copias de seguridad en este dispositivo.

Para restaurar la información del sistema del que se ha hecho copia de seguridad, utilice el mandato de CLI restore system. También se puede utilizar el mandato de CLI, diag, siempre y cuando diag esté definido como un rol de un usuario determinado.

La copia de seguridad del sistema da soporte a los métodos siguientes:

- SCP: Está definido de forma predeterminada y es accesible mediante CLI y la interfaz gráfica de usuario
- FTP: Está definido de forma predeterminada y es accesible mediante CLI y la interfaz gráfica de usuario
- Centera: Se puede añadir a la interfaz gráfica de usuario iniciando sesión en CLI y ejecutando el mandato siguiente, store storage centera backup on
- TSM: se puede añadir iniciando sesión en CLI y ejecutando el mandato siguiente, store storage tsm backup on
- AMAZON S3: Está definido de forma predeterminada y es accesible mediante CLI y la interfaz gráfica de usuario. Es accesible desde CLI siempre y cuando esté definido en la interfaz gráfica de usuario.
- Softlayer: Copia de seguridad de nube de Softlayer
- Cleversafe - funcionalidad CleverSafe: Almacenamiento de copias de seguridad de forma similar a Amazon S3. Mostrará una lista de los buckets disponibles directamente en la interfaz gráfica de usuario. El primer nombre de la lista es el nombre del bucket que se ha guardado en la base de datos. Nota: no puede crear nuevos buckets ni suprimir buckets existentes (de la CLI/interfaz gráfica de usuario de Guardium).

Nota: La restauración del sistema se debe realizar en el mismo nivel de parche de la copia de seguridad del sistema. Por ejemplo, si un cliente ha realizado una copia de seguridad del dispositivo cuando estaba en la versión 7.0, parche 7 y a continuación desea restaurar esta copia de seguridad en un dispositivo que se acaba de crear, es necesario instalar primero la versión 7.0, parches 1 a 7 en el dispositivo y sólo entonces restaurar el archivo.

Para hacer copia de seguridad de la información del sistema:

1. Pulse Gestionar > Gestión de datos > Copia de seguridad del sistema para abrir Copia de seguridad del sistema.
2. Seleccione el botón de método de almacenamiento en la lista. Según como se haya configurado el sistema Guardium, es posible que uno o más de estos botones no estén disponibles.Para ver una descripción de cómo configurar los métodos de almacenamiento de archivado y copia de seguridad, consulte la descripción para mostrar los mandatos show storage-system y store storage-system en Mandatos de CLI de configuración y control.
   - EMC CENTERA
   - TSM
   - SCP
   - FTP
   - AMAZON S3
   - Softlayer
   - Cleversafe
3. Realice el procedimiento adecuado en función del método de almacenamiento seleccionado:
   - Configurar archivado o copia de seguridad SCP o FTP
   - Configurar archivado o copia de seguridad EMC Centera
   - Configurar archivado o copia de seguridad TSM
   - Configurar archivado o copia de seguridad AMAZON S3
   - Configurar copia de seguridad de nube de Softlayer Object Storage
   - Cleversafe: Especifique> punto final válido, nombre de bucket válido, clave de acceso válida, clave secreta válida
4. Marque uno de los recuadros de selección Copia de seguridad, o ambos:
   - Marque el recuadro de selección Configuración para hacer copia de seguridad de todas las definiciones.
   - Marque el recuadro de selección Datos para hacer copia de seguridad de todos los datos. (Si archiva datos regularmente, esto no es necesario.)
5. Utilice la sección Planificación para definir una planificación para ejecutar esta operación regularmente.
6. Pulse Guardar para verificar y guardar los cambios de configuración. El sistema intentará verificar la configuración enviando un archivo de datos de prueba a esa ubicación.
   - Si la operación falla, aparece un mensaje de error y la configuración no se guardará.
   - Si la operación se realiza correctamente, la configuración se guardará.
7. Pulse Ejecutar una vez ahora para ejecutar la operación una vez.

Nota: Durante una transferencia de archivos SCP/FTP/TSM/Centera/AMAZON S3/Softlayer, si la transferencia de archivos de copia de seguridad falla, el último archivo de cada conjunto de archivos de copia de seguridad/archivado (copia de seguridad del sistema, copia de seguridad de configuración, archivado, archivado CSV, etc.) se guardará en la carpeta diag/current. A continuación, cuando el destino del archivo de copia de seguridad esté de nuevo en línea, se puede realizar una transferencia manual de los archivos de copia de seguridad desde la carpeta diag/current al destino. El conjunto de archivos de copia de seguridad/archivado sólo se guardará en la carpeta diag/current si la transferencia de archivos no se realiza correctamente. Si durante otra operación de transferencia de archivos de copia de seguridad se produce un error de transferencia de archivos, el conjunto de archivos de copia de seguridad/archivado se guardará de nuevo en la carpeta diag/current. Sin embargo, para evitar guardar demasiados archivos y que se agote el espacio de disco, SÓLO se guardará el último archivo de cada tipo. Los archivos de copia de seguridad anteriores se sobrescribirán.
Nota: Cuando se realice una copia de seguridad y restauración del sistema desde un servidor que tenga GIM definido en otro servidor, el usuario debe configurar una sustitución por anomalía de GIM en el servidor de restauración. Esta configuración de GIM se aplica a un Gestor central de copia de seguridad o a una copia de seguridad y restauración del sistema.

Archivos SCP y FTP mediante distintos puertos

Cambie los puertos que puede utilizar para enviar archivos a través de SCP y FTP.

Para Copia de seguridad del sistema o Copia de seguridad de parche: Establezca el protocolo (SCP o FTP) y especifique Host, Directorio y Puerto. El puerto predeterminado para ssh/scp/sftp es 22. El puerto predeterminado para FTP es 21.

Evitar que los scripts de copia de seguridad/archivado llenen /var

El proceso de copia de seguridad comprobará si hay espacio en /var antes de ejecutarse y fallar. Este proceso también avisará al usuario si no hay suficiente espacio para la copia de seguridad.

El proceso de archivado comprobará el tamaño de las tablas estáticas y se asegurará que haya espacio en /var para crear el archivado.

Se registra un error en el archivo de registro y la interfaz gráfica de usuario si la copia de seguridad está sobre el 50 %. Por ejemplo:

```
ERROR: Se utiliza el 60 % del espacio de copia de seguridad de /var. Espacio de disco insuficiente para la copia de seguridad.
```

Copia de seguridad y archivado Amazon S3 en Guardium

Utilice esta característica para archivar y realizar una copia de seguridad de los datos de Guardium en Amazon S3.

Amazon S3 (Amazon Simple Storage Service) proporciona una interfaz de servicio web sencilla que se puede utilizar para almacenar y recuperar cualquier cantidad de datos, en cualquier momento, desde cualquier lugar de la web. Proporciona a cualquier desarrollador acceso a la misma infraestructura altamente escalable, fiable, segura y económica que utiliza Amazon para ejecutar sus propios sitios web.

Requisitos previos

1. Una cuenta de Amazon.
2. Registro en el servicio S3
3. Se requieren credenciales de Amazon S3 para acceder a Amazon S3. Estas credenciales son:
    - ID de clave de acceso: Identifica al usuario como parte responsable de las solicitudes de servicio. Se debe incluir en cada solicitud. No es confidencial y no es necesario que esté cifrado. (secuencia alfanumérica de 20 caracteres).
    - Clave de acceso secreta: La clave de acceso secreta se asocia al ID de clave de acceso calculando una firma digital incluida en la solicitud. La clave de acceso secreta es un secreto, y sólo el usuario y AWS deberían tenerla (secuencia de 40 caracteres). Esta clave es sólo una larga serie de caracteres (y no un archivo) que se utiliza para calcular la firma digital que se debe incluir en la solicitud.

Hay dos operaciones de archivado disponibles en la consola de administración, en la sección Gestión de datos del menú:

- Archivado de datos hace copia de seguridad de los datos capturados por el dispositivo durante un periodo de tiempo determinado.
- Archivado de resultados hace copia de seguridad de los resultados de tareas de auditoría (informes, pruebas de asesoramiento, seguimiento de auditoría de entidad, conjuntos de privacidad y procesos de clasificación) así como de los seguimientos de aprobaciones y visualizaciones y los comentarios alojados de los procesos de flujo de trabajo.

Cuando se archivan los datos de Guardium, hay un archivo individual para cada día de datos.

Formato de nombre de archivo de datos de archivado:

```
 <time>-<nombre_host.dominio>-w<indicación_fecha_y_hora_ejecución>-d<fecha_datos>.dbdump.enc
```

La función de archivado crea archivos firmados y cifrados que no pueden manipularse. Los nombres de los archivos de archivado generados no se deben cambiar. La operación de archivado depende de los nombres de archivo creados durante el proceso de archivado.

Las copias de seguridad del sistema se utilizan para realizar copias de seguridad de todos los datos y valores de configuración necesarios y utilizarlos para restaurar un servidor en caso de que el hardware resulte dañado.

Toda la información y los datos de configuración se graban en un único archivo cifrado y se envían al destino especificado, utilizando el método de transferencia configurado para las copias de seguridad en este dispositivo.

Formato de archivo de sistema de copia de seguridad:

```
<fecha_datos>-<hora>-<nombre_host.dominio>-SQLGUARD_CONFIG-9.0.tgz
<fecha_datos>-<time>-<nombre_host.dominio>-SQLGUARD_DATA-9.0.tgz
```

El informe Registro de agregación/archivado se puede utilizar para verificar que la operación se completa correctamente. Debería haber varias actividades listadas para cada operación de archivado, y el estado de cada actividad debería ser Satisfactorio.

Independientemente del destino de los datos archivados, el catálogo de Guardium realiza un seguimiento de dónde se envía cada archivo de archivado, para que se pueda recuperar y restaurar en el sistema con el mínimo esfuerzo en cualquier momento en el futuro.

Se mantiene un catálogo individual en cada dispositivo, y se añade un nuevo registro al catálogo cada vez que el dispositivo archiva datos o resultados.

Las entradas de catálogo se pueden transferir entre dispositivos mediante uno de los métodos siguientes:

- Agregación: Se agregan tablas de catálogo, lo que significa que el agregador tendrá el catálogo fusionado de todos sus recopiladores
- Exportar/Importar catálogo: Estas funciones se pueden utilizar para transferir entradas de catálogo entre recopiladores, o para hacer copia de seguridad de un catálogo para su restauración posterior, etc.
- Restauración de datos: Cada operación de restauración de datos contiene los datos del día archivado, incluido el catálogo de ese día. Por lo tanto, al restaurar datos, el catálogo también se actualiza.

Cuando se importen entradas de catálogo de otro sistema, estas entradas apuntarán a archivos que ese sistema ha cifrado. Antes de restaurar o importar un archivo de este tipo, el secreto compartido del sistema correspondiente al sistema que ha cifrado el archivo debe estar disponible en el sistema de importación.

Habilite Amazon S3 desde la CLI de Guardium

La opción de copia de seguridad y archivado Amazon S3 está habilitada de forma predeterminada en la interfaz gráfica de usuario de Guardium. Para habilitar Amazon S3 mediante la CLI de Guardium, ejecute los siguientes mandatos de CLI:

```
store storage-system amazon_s3 archive on
store storage-system amazon_s3 backup on
```

Amazon S3 requiere que la hora del reloj del sistema Guardium sea correcta (menos de 15 minutos de desviación). De lo contrario, esto producirá un error de Amazon. Si hay una diferencia demasiado grande entre la hora de la solicitud y la hora actual, la solicitud no se aceptará.

Si la hora del sistema Guardium no es correcta, establezca la hora correcta mediante los siguientes mandatos de CLI:

```
show system ntp server
store system ntp server (Un ejemplo es ntp server: ntp.swg.usma.ibm.com)
store system ntp state on
```

Interfaz de usuario

Utilice la pantalla Copia de seguridad del sistema (Gestionar > Gestión de datos > Copia de seguridad del sistema) para configurar la copia de seguridad. Después de habilitar Amazon S3 mediante los mandatos de CLI, Amazon S3 aparecerá en la lista de protocolos.

La entrada de usuario requiere:

- Nombre de bucket S3 (cada objeto almacenado en Amazon S3 está contenido en un bucket. Los buckets particionan el espacio de nombres de los objetos almacenados en Amazon S3. En un bucket, puede utilizar cualquier nombre para sus objetos, pero los nombres de bucket deben ser exclusivos en todo Amazon S3.
- ID de clave de acceso
- Clave de acceso secreta

Si el nombre de bucket no existe, se creará.

La clave de acceso secreta se cifra cuando se guarda en la base de datos.

Compruebe que los archivos no se han subido en Amazon S3

1. Inicie sesión en AWS Management Console utilizando su dirección de correo electrónico y contraseña.

http://aws.amazon.com/console/

1. Pulse S3.
2. Pulse el bucket que ha especificado en la interfaz de usuario de Guardium.

Almacenamiento de objetos de Softlayer

SoftLayer Object Storage es un servicio de almacenamiento de nube altamente escalable y redundante. Utilícelo para almacenar, buscar y recuperar datos fácilmente en Internet. Se basa en la plataforma Swift de OpenStack y es accesible mediante un portal web y una API RESTful.

Información previa necesaria:

- Puntos finales de autenticación: Las solicitudes de autenticación se deben enviar al punto final asociado con la ubicación de su cuenta de Object Storage. https://dal05.objectstorage.softlayer.net/auth/v1.0
- Contenedor: La unidad de almacenamiento básica para todos los datos en Object Storage es un contenedor. Almacena datos/archivos y debe estar asociado con una cuenta de Object Storage.
- X-Auth-User: Nombre de usuario para la autenticación con: Valor arrendatario:Nombre de usuario
- X-Auth-Key: Clave de API (contraseña) para la autenticación con.

Las credenciales de cuenta se pueden recuperar iniciando sesión en https://control.softlayer.com/

Copia de seguridad del sistema de Softlayer desde la interfaz gráfica de usuario

1. Pulse Gestionar > Gestión de datos > Copia de seguridad del sistema, Gestionar > Gestión de datos > Archivado de datos o Gestionar > Gestión de datos > Archivado de resultados.
2. Seleccione el protocolo Softlayer.
3. Rellene el URL de punto final de autenticación (ejemplo, https://dal05.objectstorage.softlayer.net/auth/v1.0)
4. Especifique un nombre de contenedor de Object Storage (por ejemplo, su_nombre_contenedor)
5. Especifique X-Auth-User (Valor arrendatario: Nombre de usuario) (por ejemplo, nombre de usuario)
6. Rellene la clave X-Auth (por ejemplo, contraseña)
7. Especifique de qué se debe hacer copia de seguridad: Configuración o Datos
8. Modifique Planificación o Ejecutar una vez ahora.

Copia de seguridad del sistema mediante CLI (Configuración)

Acceda a la CLI.

CLI> sistema de copia de seguridad.

1. DATOS

2. CONFIGURACIÓN

Especifique el número de su elección: (q para salir) 1

1. SCP

2. DESTINO CONFIGURADO

Especifique el número de su elección: (q para salir) 2

Asegúrese de que el destino esté configurado en la interfaz gráfica de usuario en la opción <Copia de seguridad del sistema>

Espere, esto puede tardar algún tiempo.

Realización de una copia de seguridad PREDETERMINADA, config=

Copia de seguridad del sistema y Restauración del sistema

Acceda a la CLI.

CLI> restaurar sistema

1. SCP

2. FTP

3. TSM

4. CENTERA

5. AMAZONS3

7. SOFTLAYER

8. SFTP

Especifique el número de su elección: (q para salir) 7

Especifique el URL de punto final de autenticación de SoftLayer:

Especifique el nombre de contenedor de Softlayer Object Storage:

Especifique Softlayer X-Auth-User:

Especifique X-Auth-Key:

Especifique un nombre de archivo de la lista:

La autenticación se ha realizado correctamente.

La descarga de archivo se ha realizado correctamente.

Seleccione el tipo de recuperación; para la mayoría de los casos, utilice la opción normal:

1. normal

2. actualización

Copia de seguridad del sistema > Cleversafe

Requisito previo

El servidor de Guardium debe estar establecido en la hora local correcta. Utilice NTPserver para cambiarla, si es necesario.

Selecciones de Copia de seguridad del sistema:

URL de punto final de autenticación

Clave de acceso (AWS)

Clave de acceso secreta (AWS)

Nombre de bucket

Responda Sí a todas las preguntas sobre certificados.

Tema principal: Configuración del sistema Guardium

Configuración de la copia de seguridad de parche

Utilice esta característica para almacenar la información de perfiles de copia de seguridad.

Procedimiento

1. Pulse Configuración > Copia de seguridad de parche para abrir el panel Copia de seguridad de parche.
2. Elija el método de transferencia de archivos.
3. Especifique el nombre de host y el directorio donde se almacenará la información.
4. Especifique un nombre de usuario y una contraseña para el propietario del archivo en el host de destino.
5. Pulse Aplicar cuando haya terminado.

Tema principal: Configuración del sistema Guardium

Configurar permiso para la conexión de socket

Este tema se aplica a las clases de alertas personalizadas.

Siga este procedimiento para configurar los permisos para todas las conexiones de socket que utilizan las clases personalizadas.

1. Pulse Configuración > Evaluaciones > Permisos de comunicación para abrir los Permisos de comunicación.
2. Pulse Añadir permiso a conexión de socket para expandir ese panel.
3. Especifique la dirección IP o el nombre de host del host.
4. Especifique un número de puerto para la conexión de socket.
5. Especifique una descripción.
6. Pulse Guardar.

Tema principal: Configuración del sistema Guardium

Visión general de la gestión de acceso

La gestión de acceso consta de cuatro tareas: administración de cuentas, mantenimiento, supervisión y revocación.

La gestión de acceso no es lo mismo que las responsabilidades de administración del sistema.

Hay dos usuarios predefinidos en un dispositivo de Guardium: accessmgr y admin.

- *accessmgr* es el nombre de usuario asignado al gestor de acceso. De forma predeterminada, el gestor de acceso es el único usuario autorizado para gestionar las cuentas de usuario y los roles de seguridad.
- *admin* es el nombre de usuario asignado al administrador de Guardium (principal). De forma predeterminada, el administrador no tiene autoridad para gestionar las cuentas de usuario o roles de seguridad. El usuario de administración tiene un conjunto más amplio de privilegios.

Nota:

Los roles admin y accessmgr no se pueden asignar al mismo usuario. El mismo usuario puede contener ambos roles como resultado de una situación heredada o de una actualización. Sin embargo, el uso actual no permitirá que se asignen los dos roles al mismo usuario.

En el pasado, cuando se actualizaba una unidad, el rol accessmgr se asignaba al usuario de administración, y el usuario accessmgr se inhabilitaba. En esta situación de actualización, era necesario iniciar sesión primero como administrador y habilitar el usuario accessmgr, y a continuación iniciar sesión como accessmgr (con la contraseña inicial "accessmgr", el sistema solicitaba al usuario que la cambiara) y eliminar el rol accessmgr del usuario de administración.

Selección de la gestión de acceso

- Explorador de usuarios - Gestionar usuarios
- Explorador de roles - Gestionar permisos y personalizar diseños para roles
- Permisos de rol - Gestionar permisos de aplicación
- Importación de usuario de LDAP - Importar usuarios de LDAP

Selección de seguridad de datos

- Orígenes de datos asociados
- Orígenes de datos no asociados
- Servidores asociados
- Servidores no asociados
- Jerarquía de usuarios
- Asociación BD-usuario

Informes predefinidos de Accessmgr

Están disponibles los siguientes informes predefinidos del usuario Accessmgr.

Informes de usuarios y roles

La definición y modificación de usuarios (consulte Gestionar usuarios) implica decidir quién utilizará el sistema Guardium y a qué roles (consulte Gestionar roles) se asignarán. Un rol es un grupo de usuarios, a todos los cuales se otorgan los mismos privilegios de acceso.

Los informes de usuarios y roles constan de informes:

- Usuario - Rol: Un informe que muestra, por usuario, el número de roles al que pertenece ese usuario.
- Todos los roles - Usuario: Un informe que muestra, por rol, el número de usuarios que pertenecen a ese rol.

Nota: Los roles de administrador y gestor de acceso ya existen, los demás los crea el gestor de acceso.

En un Gestor central o una unidad autónoma están disponibles los informes siguientes. Si intenta utilizarlo en una máquina gestionada, aparecerá un mensaje de error. Servidores no asociados mostrará servidores de TODAS las unidades gestionadas en los sistemas de Gestor central.

Orígenes de datos asociados

Este informe identifica nombre de origen de datos, host, nombre de servicio, nombre de inicio de sesión y tipo de asociación. Esta información procede de las opciones realizadas en la actividad Asociaciones Usuario - Base de datos. Consulte el tema de ayuda Seguridad del usuario de datos - Jerarquía y asociaciones.

Orígenes de datos no asociados

Este informe es una lista de orígenes de datos no asociados con ningún usuario. Este informe identifica nombre de origen de datos, tipo de origen de datos, host y nombre de servicio. Esta información procede de las opciones realizadas en la actividad Asociaciones Usuario - Base de datos. Consulte el tema de ayuda Seguridad del usuario de datos - Jerarquía y asociaciones.

Servidores asociados

Este informe identifica IP de servidor, nombre de servicio, nombre de inicio de sesión y tipo de asociación. Esta información procede de las opciones realizadas en la actividad Asociaciones Usuario - Base de datos. Consulte el tema de ayuda Seguridad del usuario de datos - Jerarquía y asociaciones.

Servidores no asociados

Este informe es una lista de servidores no asociados con ningún usuario. Este informe identifica IP de servidor y nombre de servicio. Esta información procede de las opciones realizadas en la actividad Asociaciones Usuario - Base de datos. Consulte el tema de ayuda Seguridad del usuario de datos - Jerarquía y asociaciones.

- Roles
  Asigne un rol a un usuario de Guardium para otorgarle privilegios de acceso específicos. Algunos ejemplos de roles son: CLI, admin, accessmgr, CAS y user.
- Gestión de roles y permisos
  Los roles y permisos proporcionan distintos niveles de acceso a los usuarios según sus responsabilidades de trabajo.
- Cómo crear un rol con acceso mínimo
  Este tema explica cómo crear un nuevo rol con permisos de acceso mínimo, por ejemplo, un rol de auditor puede acceder sólo a la Lista de tareas pendientes de proceso de auditoría y ver informes específicos.
- Gestionar usuarios
  Utilice el gestor de acceso, que tiene asignado el nombre de usuario *accessmgr*, para añadir cuentas de usuario, habilitar o inhabilitar cuentas de usuario, importar miembros de LDAP o editar permisos de usuario. Abra el Explorador de usuarios y explore las cuentas de usuario pulsando Acceso > Gestión de acceso > Explorador de usuarios
- Cómo crear un usuario con las titularidades correctas para iniciar sesión en la CLI
  Utilice esta tarea para crear un usuario que tenga los roles y titularidades apropiados para utilizar la CLI para ejecutar mandatos de GuardAPI.
- Importación de usuarios de LDAP
  Puede importar definiciones de usuario de Guardium de un servidor LDAP configurando una operación de importación para obtener el conjunto adecuado de usuarios.
- Seguridad de datos - Jerarquía de usuarios y asociaciones de base de datos
  Puede utilizar las características de seguridad de datos para crear una jerarquía de usuarios y asociar usuarios con bases de datos y servidores específicos. Las características de seguridad de datos de Guardium notifican qué usuarios han accedido a qué información, y garantizan que sólo usuarios específicos vean la información de la que son responsables.
- Cómo definir jerarquías de usuario
  Utilice la interfaz de usuario desde una cuenta de gestor de acceso para definir fácilmente jerarquías de usuario.
- Inicio de sesión en la interfaz de usuario de Guardium mediante una tarjeta inteligente
  El soporte de tarjetas inteligentes de Guardium satisface la regulación del gobierno de Estados Unidos con relación a que todos los proveedores deben dar soporte a la autenticación de múltiples factores (MFA) para el acceso de los usuarios. El soporte de la autenticación de tarjetas inteligentes es únicamente para el acceso a la interfaz de usuario de Guardium basada en la web.

Roles

Asigne un rol a un usuario de Guardium para otorgarle privilegios de acceso específicos. Algunos ejemplos de roles son: CLI, admin, accessmgr, CAS y user.

El gestor de acceso define los roles y los asigna a usuarios y aplicaciones. Cuando se asigna un rol a una aplicación o la definición de un elemento (una consulta específica, por ejemplo), sólo los usuarios de Guardium que también estén asignados a ese rol pueden acceder a ese componente.

Cuando se importan definiciones de usuario desde un servidor LDAP, los grupos a los que pertenecen se pueden definir opcionalmente como roles. Para obtener más información, consulte Importación de usuarios de LDAP.

Nota: Cuando se asignan roles a un usuario, el rol de administración o gestor de acceso no se puede asignar el mismo usuario.
Nota: Los roles creados de forma personalizada no se pueden combinar con roles proporcionados de forma predeterminada (por ejemplo, user, admin, accessmgr, cli, inv, datasec-exempt, review-only).
Nota: De forma predeterminada, el rol de administración y el propietario de objeto tienen acceso a todos los objetos.
Nota: Si se toma un rol base y se personaliza (con elementos de navegación adicionales) y a continuación se copia este rol personalizado, si el rol personalizado o copiado se restablece a predeterminado la personalización se perderá.

Roles predeterminados

El sistema Guardium está preconfigurado para dar soporte a usuarios correspondientes a los cuatro roles predeterminados definidos globalmente: administración, usuario, gestor de acceso e investigaciones. El gestor de acceso de Guardium también puede crear nuevos roles.
Nota: Nota: si la seguridad de datos a nivel de datos observados está habilitada (consulte Ajustes de Perfil global), se permite el escalado del proceso de auditoría sólo a los usuarios en un nivel superior en la jerarquía de usuarios (consulte Gestor de acceso). El usuario Datasec-exempt se puede escalar, sin restricciones, a cualquiera.

Tabla 1. Roles predeterminados

Rol predeterminado	Descripción
user	Proporciona el diseño y acceso predeterminados para todos los usuarios comunes. Este rol no se puede suprimir.
admin	Proporciona el diseño y acceso predeterminados para los administradores de Guardium. No confunda el rol de administración con el usuario de administración, que es una cuenta de usuario especial que tiene el rol admin, pero también poderes adicionales reservados sólo a la cuenta de usuario de administración. Este rol no se puede suprimir.
accessmgr	Proporciona el diseño y acceso predeterminados para el gestor de acceso. Este rol no se puede suprimir.
cli	Proporciona acceso a la CLI. El usuario de administración tiene acceso predeterminado a la CLI. A todos los demás usuarios se les deberá otorgar permiso cuando el gestor de acceso cree usuarios y se especifiquen roles. El gestor de acceso puede definir el mismo número de usuarios en el sistema y darles el rol CLI. Estos usuarios tienen acceso a la CLI y todas las actividades de sus sesiones de CLI están asociadas con este usuario. Para ejecutar mandatos de GrdAPI o CLI sin derechos de administración, pulse el rol CLI para Consola de administración en la selección Permisos del rol de usuario. Consulte el tema, Mandato diag de CLI, sobre cómo gestionar el rol diag.

Rol predeterminado	Descripción
inv	Proporciona el diseño y el acceso predeterminados para los usuarios de investigación. Un usuario de investigación debe tener el nombre de base de datos a la que se restaurará de INV_1, INV_2 o INV_3 como apellido en su definición de usuario. No lo impone la interfaz gráfica de usuario, pero es necesario para que la aplicación funcione correctamente. Cuando está asignado, también se debe asignar el rol user. Este rol no se puede suprimir. Nota: El botón Proceso ad hoc para ejecutar una vez ahora está disponible en todas las pantallas de informe para todos los usuarios, excepto para el usuario de investigación (INV).
datasec-exempt	Seguridad de datos - Exento. Este rol se activa cuando está habilitada la seguridad a nivel de datos (consulte el Perfil global en la consola de administración) y se ha asignado el rol datasec-exempt. Si el usuario tiene este rol, aparecerá un recuadro de selección Mostrar todo en todos los informes. Si está seleccionado, se muestran todos los registros de datos detectados (no se aplica ningún filtro). Este rol no se puede suprimir en el Explorador de roles.
review-only	Un usuario especificado por este rol sólo puede ver resultados (Auditoría, Asesoramiento, Clasificador), Resultados de auditoría y la Lista de tareas pendientes. Este rol no se puede suprimir en el Explorador de roles. Los usuarios con este rol pueden especificar comentarios en el visor de procesos de auditoría (no flujo de trabajo ni comentarios/datos por fila, sino comentarios a nivel de resultado/resultado). Los usuarios con este rol no pueden realizar cambios/acciones en ningún resultado de automatización de flujo de trabajo (escalar, reasignar, etc).

Roles de ejemplo

Además de los roles predeterminados, también se define un conjunto de roles de ejemplo.

Tabla 2. Roles de ejemplo

Rol de ejemplo	Descripción
dba	Usuarios que tienen una vista de seguridad basada en bases de datos, lo que permite el acceso a los informes relacionados con base de datos y el seguimiento de objetos de base de datos.
infosec	Usuarios centrados en la seguridad de la información, lo que incluye el seguimiento del acceso a la base de datos, así como el manejo de solicitudes, auditorías y análisis forenses
netadm	Usuarios que tienen una vista basada en la red, que incluye los orígenes de IP para las solicitudes de base de datos
appdev	Desarrolladores, arquitectos y personal de control de calidad de aplicaciones que se centran en las aplicaciones y desean realizar un seguimiento e informar sobre las secuencias de SQL generadas por una aplicación
audit	Auditores y otros que necesitan ver los informes de auditoría Nota: Si intenta copiar este rol, aparecerá un mensaje incorporado que explicará que no se pueden copiar todos los aspectos de este rol. El mensaje es: "Cree un rol nuevo utilizando el diseño y permiso del rol "audit". Los privilegios y acciones especiales asociados con el rol "audit" no se copiarán."
audit-delete	Este rol se utiliza para realizar el seguimiento o registrar cuando se ha suprimido un resultado de proceso de auditoría. Los usuarios con el rol audit-delete pueden suprimir informes. Los usuarios de administración también pueden suprimir informes. El seguimiento se realiza mediante el informe Seguimiento de auditoría de actividad de usuario.
admin-console-only	Un usuario especificado por este rol puede acceder sólo al separador de la consola de administración.
cas	CAS (Configuration Auditing System)
vulnerability-assess	Un usuario especificado por este rol puede ver sólo resultados de vulnerabilidades.
diag	Un usuario especificado por este rol puede acceder y ejecutar los mandatos diag en la CLI.
workload-replay-admin	Un usuario especificado por este rol puede definir y modificar las funciones de reproducción de carga de trabajos.
workload-replay-user	Un usuario especificado por este rol puede ejecutar las funciones de reproducción de carga de trabajo.
fam	Un usuario especificado por este rol puede definir y modificar las funciones de supervisión de actividad de archivos.
BaselII	Accelerator - Basel II. Este rol no se puede suprimir. Según las secciones 4 y 5, parte 2, del convenio de Basilea II se requiere que las instituciones bancarias definan una infraestructura de seguridad de la información financiera y estimen los riesgos operativos asociados.
DataPrivacy	Accelerator - DataPrivacy. Este rol no se puede suprimir. Data Privacy Accelerator proporciona un portfolio de políticas preconfiguradas, alertas en tiempo real e informes de auditoría que están especialmente personalizados para los retos de robo de identidad y que se basan en las mejores prácticas del sector. Con Data Privacy Accelerator, los gestores de seguridad, los agentes de privacidad y los administradores de bases de datos empiezan definiendo combinaciones de elementos de datos, llamados "conjuntos de privacidad", cuyo acceso puede indicar hackeado o actividades inadecuadas por parte de usuarios internos.
GDPR	Accelerator - GDPR. Este rol no se puede suprimir. Guardium GDPR Accelerator proporciona informes predefinidos basados en grupos y políticas de GDPR. Para empezar a trabajar con GDPR Accelerator, asigne el rol GDPR a un usuario de Guardium y a continuación vaya a Accelerators > GDPR con la cuenta de usuario.
pci	Accelerator - PCI. Este rol no se puede suprimir. PCI DSS es un conjunto de requisitos técnicos y operativos diseñados para proteger los datos del titular de la tarjeta y que se aplican a todas las organizaciones que almacenan, procesan, utilizan o transmiten datos de titulares de tarjetas. Si no se cumple este conjunto de requisitos, significa la pérdida de privilegios, multas severas y, en caso de una filtración de datos, pérdida grave de la confianza del consumidor en su marca o servicios. IBM Guardium Accelerator le guía por el proceso de cumplimiento con partes del estándar utilizando políticas, informes y definiciones de grupo predefinidos, y otros.

Rol de ejemplo	Descripción
sox	Accelerator - SOX. Este rol no se puede suprimir. La sección 404 de SOX requiere que las empresas establezcan y mantengan una estructura de control interno y procedimientos adecuados para la creación de informes financieros.

Roles de un entorno de Gestor central

En entornos de Gestor central, todas las cuentas de usuario, todos los roles y todos los permisos los controla el Gestor central. Para administrar cualquiera de estas definiciones, debe iniciar sesión en el Gestor central (no en una unidad gestionada).

Crear un rol

1. Inicie sesión como accessmgr y abra el Navegador de rol de usuario pulsando Acceso > Gestión de acceso > Explorador de roles.
2. Pulse Añadir rol para abrir el panel Formulario de roles.
3. Especifique un nombre exclusivo para Nombre de rol y pulse Añadir rol.

Eliminar un rol

1. Abra el Navegador de rol de usuario pulsando Acceso > Gestión de acceso > Explorador de roles.
2. Pulse Suprimir para cualquier rol (algunos roles no se pueden eliminar, y no tienen la opción Suprimir). Esto abre el Formulario de roles para el rol.
3. Pulse Confirmar la acción de suprimir. Se visualiza un mensaje que le informa que se han eliminado todas las referencias al rol, y se le solicitará que confirme la acción.
4. Pulse Aceptar para confirmar la supresión, o Cancelar para terminar anormalmente la operación.

Tema principal: Visión general de la gestión de acceso

Gestión de roles y permisos

Los roles y permisos proporcionan distintos niveles de acceso a los usuarios según sus responsabilidades de trabajo.

Ejemplos de roles son usuario, administrador y auditoría. La utilización de roles le permite definir fácilmente permisos para todo un grupo de usuarios. Sólo los gestores de acceso pueden crear nuevos roles y asignar usuarios a ese rol. Como parte de la creación de roles, los gestores de acceso pueden personalizar el menú de navegación y los permisos para ese rol.

La creación de roles personalizados implica varios procesos:

- Creación de un nuevo rol
- Gestión de permisos para el rol para limitar a qué pueden acceder los usuarios
- Opcionalmente, personalización del menú de navegación para el rol para limitar adicionalmente lo que los usuarios pueden ver
- Adición de usuarios al rol

Hay dos maneras de limitar el acceso a aplicaciones específicas:

Limite el acceso desde la aplicación

Limite el acceso desde la aplicación desmarcando el recuadro de selección Todos los roles de la pantalla Permisos de rol > Editar permisos del rol de aplicación. A continuación, seleccione los roles individuales que deberían acceder a la aplicación.

El proceso es el mismo si encuentra que el recuadro de selección Todos los roles ya está desmarcado: simplemente marque o desmarque los roles individuales para otorgar o revocar acceso a la aplicación.

Cuando está seleccionado Todos los roles para una aplicación determinada, cada rol definido actualmente tendrá acceso a esa aplicación.

Limite el acceso desde el rol

Para limitar el acceso desde el rol vaya a la pantalla Navegador de roles > Gestionar permisos y mueva aplicaciones individuales de la lista Aplicaciones accesibles a la lista Aplicaciones inaccesibles.

Cuando se gestionan permisos o se personaliza el menú de navegación para un rol nuevo, los valores predeterminados que se muestran en la lista Aplicaciones accesibles reflejan cualquier aplicación con el recuadro de selección Todos los roles seleccionada en la pantalla Permisos de rol > Editar permisos del rol de aplicación.

Cuando se trabajan con roles y permisos, al eliminar permisos de una aplicación también cambian los permisos predeterminados para los roles nuevos. Es decir, cuando se eliminan permisos para una aplicación, cualquier rol subsiguiente que se cree también carecerá de permisos para esa aplicación. Si desea que un rol nuevo tenga permisos para una aplicación que ya no aparece de forma predeterminada en la lista Aplicaciones accesibles, deberá mover la aplicación que desee de la lista Aplicaciones inaccesibles a la lista Aplicaciones accesibles del nuevo rol.

También es posible restringir el acceso a herramientas específicas ocultando elementos de menú mediante la herramienta Navegador de roles > Personalizar menú de navegación. Este enfoque limita el acceso sin alterar los permisos predeterminados de la aplicación, pero puede ser menos seguro que un enfoque basado en permisos.

Mejores prácticas:

- Tras editar los permisos de un rol, revise el diseño de navegación de ese rol tal como se muestra en la pantalla Navegador de roles > Personalizar menú de navegación. Añada o elimine elementos de la lista Menú de navegación tal como se requiere para crear un diseño adecuado para el rol.
- Copie y edite los roles predefinidos para establecer los permisos y el menú de navegación que desea. Este enfoque le permite revertir el rol original, si así se requiere.

Tema principal: Visión general de la gestión de acceso
Tareas relacionadas:
Cómo crear un rol con acceso mínimo
Información relacionada:

Personalización de la interfaz de usuario
Gestión de usuarios, roles y del sistema Guardium (vídeo)

Cómo crear un rol con acceso mínimo

Este tema explica cómo crear un nuevo rol con permisos de acceso mínimo, por ejemplo, un rol de auditor puede acceder sólo a la Lista de tareas pendientes de proceso de auditoría y ver informes específicos.

Procedimiento

1. Cree un rol nuevo.
   a. Inicie sesión como *accessmgr*, vaya a Acceso > Gestión de acceso y seleccione Explorador de roles.
   b. Pulse el botón Añadir rol, proporcione al rol un nombre y pulse el botón Añadir rol para crear el nuevo rol.
2. Gestione permisos de forma que el nuevo rol sólo pueda acceder a la Lista de tareas pendientes de proceso de auditoría y al Creador de informes (necesario para visualizar los informes).
   a. En el Explorador de roles, pulse el enlace Gestionar permisos para el nuevo rol.
   b. Marque el recuadro de selección en la cabecera de la lista Elementos accesibles y utilice la flecha para mover todos los elementos a la lista Elementos inaccesibles. Cuando se crea un rol muy restringido, resulta más fácil empezar eliminando permisos.
   c. En la lista Elementos inaccesibles, seleccione la Lista de tareas pendientes de proceso de auditoría y el Creador de informes y utilice la flecha para moverlos de nuevo a la lista Elementos accesibles. El nuevo rol ahora tiene acceso sólo a estas dos aplicaciones específicas.
   d. Pulse el botón Aceptar para confirmar los cambios.
3. Personalice los menús y la navegación definiendo qué informes y aplicaciones estarán disponibles para el nuevo rol.
   a. En el Navegador de roles, pulse el enlace Personalizar menú de navegación para el nuevo rol.
   b. En la lista Menú de navegación seleccione el grupo Informes de manera que quede resaltado. El grupo seleccionado actúa como destino de los elementos de menú añadidos en los pasos posteriores.
   c. En la lista Herramientas e informes disponibles, expanda la sección Informes o utilice el Filtro para identificar informes específicos, marque el recuadro de selección junto a cada elemento que debe estar disponible al nuevo rol, y utilice la flecha para añadir los elementos a la lista Menú de navegación. Los elementos que se han movido a la lista Menú de navegación se visualizarán a los usuarios asignados a este rol.
   d. En la lista Menú de navegación, elimine el acceso al Creador de informes pulsando los iconos junto a los grupos Informes > Herramientas de configuración de informes e Investigar. Esto simplifica adicionalmente la estructura de menús para este rol y elimina el acceso a la herramienta Creador de informes sin eliminar también los permisos de aplicación necesarios para acceder a los informes.
   e. Pulse el botón Aceptar para confirmar los cambios. Ahora ha creado un nuevo rol con privilegios muy mínimos que se pueden asignar a los usuarios.
4. Opcionalmente, especifique una página de inicio personalizada para el nuevo rol.
   a. En el Navegador de roles, pulse el enlace Personalizar menú de navegación para el nuevo rol.
   b. En la lista Menú de navegación, especifique una nueva página de inicio predeterminada seleccionando Cumplir > Herramientas y vistas > Lista de tareas pendientes de proceso de auditoría y pulsando el icono de la barra de herramientas. Los usuarios asignados a este rol ahora verán la Lista de tareas pendientes de proceso de auditoría como la pantalla predeterminada tras el inicio de sesión.
   c. Pulse el botón Aceptar para confirmar los cambios.
5. Cree un nuevo usuario y añada ese usuario al nuevo rol.
   a. Vaya a Acceso > Gestión de acceso y seleccione Explorador de usuarios.
   b. Pulse Añadir usuario, proporcione la información necesaria y pulse Añadir usuario para crear el nuevo usuario. Ahora verá que el usuario que ha creado se lista en el Explorador de usuarios.

      Cuando se crea un usuario nuevo, de forma predeterminada la cuenta está inhabilitada. Desmarque el recuadro de selección Inhabilitado si desea que el usuario tenga acceso inmediato a su cuenta.

   c. En el Explorador de usuarios, pulse el enlace Roles para que el nuevo usuario vea una lista de roles disponibles.
   d. Marque el recuadro de selección Asignar junto al rol personalizado que ha creado anteriormente. Esto asignará el usuario al nuevo rol.
   e. Desmarque el recuadro de selección Asignar junto al rol de *usuario*. Si se desmarca el rol *usuario*, el nuevo usuario no heredará el acceso ni los permisos predeterminados de *usuario*.
   f. Pulse Guardar para confirmar los cambios.

Tema principal: Visión general de la gestión de acceso
Conceptos relacionados:
Gestión de roles y permisos

Gestionar usuarios

Utilice el gestor de acceso, que tiene asignado el nombre de usuario *accessmgr*, para añadir cuentas de usuario, habilitar o inhabilitar cuentas de usuario, importar miembros de LDAP o editar permisos de usuario. Abra el Explorador de usuarios y explore las cuentas de usuario pulsando Acceso > Gestión de acceso > Explorador de usuarios

La definición y modificación de usuarios implica decidir quién utilizar el sistema Guardium y a qué roles se asignarán. Los usuarios de un grupo de usuarios pueden tener todos el mismo rol y los mismos privilegios de acceso, si así lo elige. Para obtener más información sobre los roles, consulte Roles.

Nota: Se puede definir un diseño predeterminado para un rol, de modo que cualquier usuario asignado a ese rol tendrá ese diseño. Consulte Generar diseño nuevo en la Referencia de la CLI.

Se pueden importar definiciones de usuario desde un servidor LDAP, a petición o de forma planificada.

Independientemente de cómo se definan los usuarios en el sistema Guardium, el administrador de Guardium puede configurar el sistema para autenticar usuarios mediante Guardium, LDAP o Radius.

Cuando empiece a utilizar el sistema Guardium, una tarea importante que debe realizar al principio es identificar qué grupos de usuarios utilizarán el sistema, y cuál será su función. Por ejemplo, un grupo de seguridad de información podría utilizar Guardium para alertas y para la resolución de problemas, mientras que un administrador de base de datos podría utilizar Guardium para informes y la supervisión. Cuando decida quién accederá al sistema Guardium, tenga en cuenta que el sistema puede recoger información confidencial de la empresa. Por lo tanto, tenga mucho cuidado sobre quién podrá acceder a esos datos.

Una vez que decida qué grupos de usuarios podrán utilizar el sistema Guardium (y para qué finalidad), recopile la siguiente información para cada usuario:

- El nombre y apellido del usuario
- El nombre de cuenta del usuario (el nombre que utilizarán para iniciar sesión)
- La dirección de correo electrónico del usuario
- La función/rol del usuario con Guardium

Seguridad de cuentas de usuario

Se pueden modificar varios valores para proporcionar seguridad adicional para las cuentas de usuario. Puede habilitar o inhabilitar estos valores utilizando los mandatos de CLI show password y store password (consulte los mandatos de CLI de Cuenta de usuario, Contraseña y Autenticación en la Referencia de la CLI).

- De forma predeterminada, la validación de contraseña está habilitada. Esto significa que se requiere un mínimo de ocho caracteres, y la contraseña debe contener al menos un carácter de cada una de las categorías siguientes:
  - Letras mayúsculas: A-Z
  - Letras minúsculas: a-z
  - Dígitos: 0-9
  - Caracteres especiales: @#$%^&.;!-+=_

  Nota: Si la validación de contraseña está inhabilitada, se permite cualquier carácter.
- De forma predeterminada, la caducidad de contraseña está habilitada. Las contraseñas se pueden configurar para que caduquen tras un número indicado de días.
- De forma predeterminada, el bloqueo de cuenta que sigue a un número especificado de intentos fallidos de inicio de sesión está habilitado. Se puede configurar el bloqueo para que se produzca tras un número especificado de intentos en un periodo de tiempo determinado, o tras un número total de intentos durante la vida de la cuenta.

Cuentas bloqueadas

1. Abra el Explorador de usuarios pulsando Acceso > Gestión de acceso para ver la lista de usuarios.
2. Pulse Editar para cualquier usuario, desmarque el recuadro de selección Inhabilitado y pulse Actualizar usuario para guardar los cambios.
   Nota: Si la cuenta de usuario de administración se bloquea, utilice el mandato de CLI unlock admin para desbloquearla (consulte los mandatos de CLI de configuración y control en la Referencia de la CLI).

Crear una cuenta de usuario

1. Abra el Explorador de usuarios y pulse Añadir usuario para abrir el panel Formulario de usuario.
2. Especifique un nombre exclusivo para Nombre de usuario. No incluya apóstrofos en el nombre. Los nombres de usuario no son sensibles a mayúsculas y minúsculas.
   Nota: Cuando añade un usuario manualmente, desde el panel Añadir usuario o desde Importar usuarios LDAP, si no hay ningún nombre y/o apellido se utilizará el nombre de inicio de sesión.
3. Especifique una contraseña y confírmela de nuevo en el recuadro Contraseña (confirmar). La contraseña que asigne será temporal, y el usuario deberá cambiarla tras el primer inicio de sesión.
   Nota: Las contraseñas no son sensibles a mayúsculas y minúsculas. Cuando la validación de contraseña está habilitada (el valor predeterminado), la contraseña debe tener una longitud de ocho o más caracteres y debe incluir al menos un carácter alfabético en mayúsculas (A-Z), un carácter alfabético en minúsculas (a-z), un dígito (0-9) y un carácter especial del conjunto siguiente: @$%^&.;!-+=_
   Nota: En el nombre de usuario no se da soporte a los caracteres no latinos, por ejemplo, los caracteres japoneses o chinos.
4. Especifique el nombre y apellido del usuario en sus campos respectivos.
   Nota: Se aplican restricciones al apellido de los usuarios asignados al rol Restaurar los datos de investigación (inv). Si desea asignar un usuario al rol de investigador, su apellido debe ser INV_1, INV_2, INV_3. La interfaz de usuario no le impedirá que especifique algo diferente en este campo, pero la aplicación no funcionará correctamente a menos que se especifique el apellido tal como se muestra. Además, no se puede asignar al investigador roles adicionales, sólo pueden ser inv. Este es el único caso donde no se requiere tener un rol user o admin.
5. (Opcional) Especifique la dirección de correo electrónico del usuario.
6. (Precaución) De forma predeterminada, el recuadro de selección Inhabilitado está marcado. Sugerimos que aplace desmarcar el recuadro de selección y habilitar la cuenta hasta después de que se haya asignado el conjunto de roles correcto al usuario.

   Es mucho más sencillo asignar primero los roles, de manera que el usuario tenga todos los componentes en su diseño la primera vez que inicie sesión. Cuando un usuario inicia sesión por primera vez, sus diseños se crean utilizando todos los roles asignados en ese momento. Si se añaden roles posteriormente, el usuario tiene acceso a todo lo que está disponible a ese rol, pero deberá añadir manualmente los informes o aplicaciones específicos de ese rol.
7. Pulse Añadir usuario para guardar la nueva definición de cuenta de usuario y cerrar el panel.

Esto completa la definición de usuario. Sugerimos que añada los roles adecuados para el usuario antes de informarle sobre su contraseña para el inicio de sesión inicial. Consulte Roles para obtener más información.

Habilitar/inhabilitar muchos usuarios

Abra el Navegador de usuarios y pulse Buscar usuarios para filtrar fácilmente los usuarios por rol. Cuando selecciona un usuario, tiene la opción de habilitar o inhabilitar el usuario. Puesto que de forma predeterminada los usuarios están inhabilitados, este menú puede resultar útil para cambiar fácilmente el estado de muchos usuarios.

Actualizar una cuenta de usuario

1. Abra el Explorador de usuarios y pulse Editar para el usuario que desea modificar.
2. Reemplace los valores del panel Formulario de usuario.
3. Pulse Actualizar usuario para guardar los cambios.

Nota: Para cambiar la contraseña de un usuario será necesario que el usuario la cambie tras su siguiente inicio de sesión.

Habilitar una cuenta de usuario inhabilitada

1. Abra el Explorador de usuarios y pulse Editar para el usuario que desea habilitar.
2. Desmarque el recuadro de selección Inhabilitado.
3. Si el usuario ha olvidado su contraseña, especifique una nueva contraseña en los recuadros Contraseña y Contraseña (confirmar).
4. Pulse Actualizar usuario.

Eliminar una cuenta de usuario

1. Abra el Explorador de usuarios pulsando Acceso > Gestión de acceso.
2. Pulse Suprimir para el usuario que desea eliminar.
3. Pulse Confirmar la acción de suprimir.

Nota: Las alertas enviadas al usuario suprimido se enviarán ahora al usuario de administración, pero esto no se aplicará hasta que se haya reinstalado la política de acceso.

Definir la jerarquía de usuarios de seguridad de datos

1. Pulse Seguridad de datos > Jerarquía de usuarios.
2. Seleccione un usuario en el menú Usuario para renovar la pantalla y mostrar la jerarquía actual del usuario seleccionado en el panel del usuario.
3. Pulse con el botón derecho del ratón un nodo de usuario para la siguiente operación:
   - Añadir usuario: Al pulsar Añadir usuario se muestra el diálogo Añadir usuario. Busque o filtre por rol, y añada un usuario como descendiente del usuario seleccionado.

     Esto puede crear una medida de seguridad a nivel de datos, permitiendo que el padre de la jerarquía vea los servidores y bases de datos especificados, pero no los hijos de la jerarquía. En función de la configuración, la herencia también puede tener lugar cuando el padre hereda la seguridad a nivel de datos del hijo.

     Nota: Se permiten relaciones "de varios a varios" cuando un usuario puede tener más de un padre y un padre puede tener más de un usuario.
   - Deshacer el enlace de usuario desde padre: Separará el descendiente del padre
   - Eliminar todos los descendientes: Separará todos los descendientes del padre
4. Pulse Renovar la jerarquía en caché para aplicar los cambios recientes a la correlación de la jerarquía de usuarios.
5. Pulse Actualización completa de correlaciones de usuario-base de datos para aplicar completamente todos los cambios recientes a las correlaciones de usuario-BD activas.
   Nota: Las mejores prácticas dictan una Actualización completa de correlaciones de usuario-base de datos tras cambiar la jerarquía de usuarios.

   Cuando realice un cambio en la jerarquía o en una asociación de base de datos (mediante la interfaz de usuario o GuardAPI), este cambio NO se aplica automáticamente. La actualización periódica NO recogerá este cambio, a menos que sea la PRIMERA vez que se ejecuta la actualización periódica. De lo contrario, el usuario DEBE pulsar Actualización completa o ejecutar el mandato de GuardAPI de actualización completa para que se apliquen sus cambios.

   Una actualización periódica de la jerarquía de usuarios se ejecuta automáticamente cada 10 minutos. Esto no se puede ejecutar manualmente. Se trata de una actualización incremental, lo que significa que sólo examina las IP de servidor o nombres de servicio nuevos que se han detectado desde la última vez que se ejecutó la actualización periódica. Compara la jerarquía y las asociaciones existentes con las nuevas IP/nombres de servicio y determina qué usuarios deben tener acceso a estas IP/nombres de servicio.

   Una actualización completa de la jerarquía de usuarios NO se ejecuta automáticamente. Sólo se ejecuta cuando el usuario la ejecuta, ya sea mediante la interfaz de usuario o mediante la función de GuardAPI. Esto compara TODAS las IP/TODOS los nombres de servicio con la jerarquía y asociaciones existentes para determinar quién tiene acceso a qué.

Definir la asociación de usuario de seguridad de datos a base de datos

Utilice la asociación BD-usuario de seguridad de datos para buscar, asignar o eliminar usuarios de los servidores y nombres de servicio (bases de datos) disponibles.

1. Abra el panel Asociación BD-usuario pulsando Seguridad de datos > Asociación BD-usuario.
2. Marque los recuadros de selección de Sugerencias de nombres de servicio y servidores para buscar bases de datos y nombres de servicio para asociar a los usuarios. Las opciones incluyen:
   - Accesos observados: Tráfico observado desde la tabla de base de datos interna de Guardium GDM_Access
   - Definiciones de orígenes de datos: Información de definición de origen de datos existente como, por ejemplo, nombre, tipo de base de datos, información de autenticación y ubicación de origen de datos.
   - Definiciones de S-TAP: Información de definición de S-TAP existente como, por ejemplo, la dirección IP del servidor de base de datos y la dirección IP del host de Guardium que recibirá datos de S-TAP.
   - Hosts de descubrimiento automático: Hosts descubiertos por el proceso de descubrimiento automático de Guardium que no se conocían anteriormente. Se puede configurar la aplicación de autodescubrimiento de Guardium para sondear la red, buscando bases de datos e informando sobre todas las bases de datos descubiertas.
   - Sistemas descubiertos de GIM (Guardium Install Manager): Los hosts que ha descubierto GIM que no se conocían anteriormente.
3. Pulse Ir para buscar y mostrar los servidores y nombres de servicio disponibles y los usuarios asociados actualmente.
   Nota: Cuando se atraviesa el árbol de nodos, se muestran indicadores numéricos junto a cada servidor y nombre de servicio para proporcionar un recuento de los usuarios directos y descendientes que se han asociado. Los indicadores tienen el formato [nn] para la asociación directa y (mm) para la asociación de descendiente (por ejemplo, un servidor o nombre de servicio en el servidor actual tiene un usuario asociado). De la misma forma, cuando se visualizan los usuarios asociados a un servidor o nombre de servicio, si hay un usuario asociado a un nodo de nivel mayor del árbol, se mostrará ese usuario.
4. Pulse un nodo de servidor o nombre de servicio para visualizar los usuarios asociados. Con cualquier nodo seleccionado, puede realizar una de las acciones siguientes:
   - Pulse Añadir usuario para añadir una nueva asociación BD-usuario, pulse cualquier usuario que desee añadir y a continuación pulse Añadir.
   - Pulse Añadir grupo para añadir una nueva asociación BD-grupo. Cuando Añadir grupo esté seleccionado, se mostrarán los grupos creados utilizando el Creador de grupos para el tipo de grupo Usuarios de Guardium. Seleccione el grupo que desea añadir y pulse Añadir.
   - Pulse con el botón derecho en cualquier servidor o nombre de servicio para realizar una de las acciones siguientes:
5. Pulse con el botón derecho del ratón cualquier nodo de servidor o nombre de servicio y se le presentarán las opciones para hacer lo siguiente:
   - Resaltar el servidor
   - Expandir o contraer el servidor
   - Buscar un servidor
   - Añadir servidor, nombre de servicio o servicio sin nombre
   - Suprimir el servidor
6. Añada una IP o un par IP/nombre de servicio utilizando los campos IP y Nombre de servicio antes de la estructura de árbol.
   Nota: El botón Encontrar se puede utilizar para buscar la estructura de árbol de IP/nombre de servicio. Las series de IP se pueden especificar como parciales o incluir el comodín *, de forma que tanto 192.168 como 192.168.*.* son válidas. Los valores numéricos no pueden finalizar con el uso de un comodín o utilizarse con el comodín para formar un octeto. Los nombres de servicio pueden incluir el comodín % en cualquier lugar de su nombre.
7. Pulse Actualización completa de correlaciones de usuario-base de datos para aplicar completamente todos los cambios recientes a las correlaciones de usuario-BD activas.

Nota: Las mejores prácticas dictan una actualización completa de la correlación de usuario-BD activa tras cambiar la asociación de BD-usuario.

Una actualización completa de la jerarquía de usuarios NO se ejecuta automáticamente. Sólo se ejecuta después de que la ejecute el usuario, mediante el botón Actualización completa de correlaciones de usuario-base de datos o la función de GuardAPI. Esto compara TODAS las IP/TODOS los nombres de servicio con la jerarquía y asociaciones existentes para determinar quién tiene acceso a qué.

Se ejecuta automáticamente una actualización periódica de la jerarquía de usuarios cada 10 minutos (no se puede ejecutar manualmente). Esta actualización sólo examina las IP de servidor o nombres de servicio nuevos que se han detectado desde la última ejecución de la actualización periódica. Compara la jerarquía y las asociaciones existentes con las nuevas IP/nombres de servicio y determina qué usuarios deben tener acceso a estas IP/nombres de servicio.

Cuando realiza un cambio en una asociación de base de datos (mediante la interfaz de usuario o GuardAPI), este cambio NO se aplica automáticamente. La actualización periódica NO recogerá este cambio, a menos que sea la PRIMERA vez que se ejecuta la actualización periódica. De lo contrario, el usuario DEBE pulsar el botón Actualización completa de correlaciones de usuario-base de datos o ejecutar el mandato GuardAPI de actualización completa para que se apliquen los cambios.

Tema principal: Visión general de la gestión de acceso

Cómo crear un usuario con las titularidades correctas para iniciar sesión en la CLI

Utilice esta tarea para crear un usuario que tenga los roles y titularidades apropiados para utilizar la CLI para ejecutar mandatos de GuardAPI.

Acerca de esta tarea

Este tema de procedimiento es importante ya que (1) los mandatos de GuardAPI se pueden ejecutar sólo mediante la CLI, y (2) la mayoría de los mandatos de GuardAPI están asociados con una aplicación específica y, por lo tanto, con sus roles, lo que significa que el usuario estándar de la CLI (que tiene un rol "admin" codificado) no puede ejecutar muchos de los mandatos GuardAPI porque ese usuario no tiene los roles adecuados.

Procedimiento

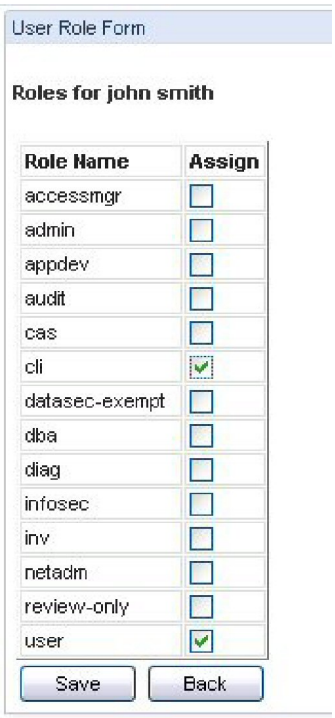
1. Inicie sesión como accessmgr y abra el Explorador de usuarios pulsando Acceso > Gestión de acceso > Explorador de usuarios.
2. Pulse Añadir usuario en el panel Explorador de usuarios.

3. Rellene el Formulario de usuario, desmarque el recuadro de selección Inhabilitado para habilitar el usuario cuando se cree, y pulse Añadir usuario.

Cuando se crea inicialmente un usuario, este no tiene privilegio para iniciar sesión en la CLI ni para ejecutar los mandatos de GuardAPI. Como ejemplo, si intentamos utilizar una de las cuentas de la CLI (guardcli1,...,guardcli5) con el usuario que se acaba de crear, se nos desconecta rápidamente y se indica que el usuario no tiene definido el rol necesario.

```
$ ssh -l guardcli1 192.168.1.89  guardcli1@192.168.1.89's password:
Last login: Tue Aug 10 18:37:25 2010 from 192.168.1.14
Welcome guardcli1 - your last login was Tue Aug 10 18:37:26 2010
Please enter your GUI login (one with ADMIN or CLI role defined):johnsmith
No such user or user does not have the necessary role defined.
Connection to 192.168.1.89 closed.
```

4. En el panel Explorador de usuarios, pulse Roles para cualquier usuario para que aparezca el panel Formulario de rol de usuario.
5. Marque el recuadro de selección CLI y pulse Guardar para otorgar al usuario acceso a la CLI.



Ahora cuando el usuario intenta utilizar una de las cuentas de la CLI (guardcli1,...,guardcli5) con el usuario que se acaba de crear, se le solicita una contraseña y se le otorga acceso a la CLI.

```
$ ssh -l guardcli1 192.168.1.89
guardcli1@192.168.1.89's password:
Last login: Tue Aug 10 18:39:01 2012 from 192.168.1.14
Welcome guardcli1 - your last login was Tue Aug 10 18:39:02 2011
The 'set guiuser' command must be run (successfully) before any other commands will work
set guiuser admin
Enter current password
192.168.1.89>
```

6. Otorgue roles adicionales, si así lo desea, para permitir acceso al usuario para ejecutar funciones de GuardAPI.

   Por ejemplo, si el usuario johnsmith fuera a emitir el siguiente mandato de GuardAPI, encontraría que no tiene ningún mandato de API para ejecutar:

   ```
   192.168.1.89 >grdapi commands user
   ID=0
   Matching API Function list:
   ok
   ```

   Pero, si fuera a otorgar a johnsmith el rol accessmgr (anteriormente en el paso 5), el mismo mandato de GuardAPI haría que estuvieran disponibles los siguientes mandatos de la API:

   ```
   192.168.1.89> grdapi commands user
   ID=0  Matching API Function list :
   create_db_user_mapping
   create_user_hierarchy
   delete_allowed_db_by_user
   delete_db_user_mapping
   delete_user_hierarchy_by_entry_id
   delete_user_hierarchy_by_user
   execute_ldap_user_import
   list_allowed_db_by_user
   list_db_user_mapping
   list_user_hierarchy_by parent_user
   update_user_db
   ok
   ```

Tema principal: Visión general de la gestión de acceso

Importación de usuarios de LDAP

Puede importar definiciones de usuario de Guardium de un servidor LDAP configurando una operación de importación para obtener el conjunto adecuado de usuarios.

Puede ejecutar la operación de importación bajo demanda, o planificarla para que se ejecute periódicamente. Puede optar por importar nuevos usuarios o sustituir las definiciones de usuario existentes. En cualquiera de los dos casos, los grupos LDAP se pueden importar como roles de Guardium.

Cuando se importan usuarios de LDAP:

- La definición de usuario de administración de Guardium no cambiará de ninguna forma.
- Los usuarios existentes no se suprimirán (en otras palabras, el conjunto importado desde LDAP no sustituye todo el conjunto de usuarios).
- Las contraseñas de Guardium no cambiarán.
- Los nuevos usuarios añadidos a Guardium:
  - Se marcarán como inactivos de forma predeterminada

- Tendrán contraseñas en blanco
- Se les asignará el rol de usuario

Nota:

No se permiten caracteres especiales en un nombre de usuario.

Cuando se añade un usuario manualmente mediante Gestión de acceso (desde Añadir usuario o desde Importar usuarios LDAP), si no hay ningún nombre y/o apellido, se utilizará el nombre de inicio de sesión.

Esta pantalla del menú de configuración de LDAP tiene ayuda contextual para determinadas opciones del menú. Mueva el cursor sobre una opción de menú (por ejemplo, Clase de objeto para usuario), y aparecerá una breve descripción.

Los usuarios de la CLI de Guardium no se pueden autenticar en el entorno de LDAP, ya que no hay ninguna separación de privilegios para los usuarios de la CLI.

Configurar Importar usuarios LDAP

Se utilizará el atributo para identificar los usuarios definidos por el administrador de Guardium, en el recuadro Tipo de RDN de usuario del panel Configuración de autenticación LDAP. Consulte Configurar autenticación LDAP para obtener información adicional. El valor predeterminado es uid, pero debe consultar con el administrador de Guardium para determinar qué valor se utiliza. Si el usuario utiliza SamAccountName como valor de RDN, el usuario debe utilizar a =search o =[nombre de dominio] en el nombre completo. Ejemplos: SamAccountName=search, SamAccountName=dom

Nota: Para configurar la importación de usuario de LDAP, el usuario accessmgr debe tener el privilegio para ejecutar Creador de grupos. En determinadas situaciones, cuando se realizan cambios en el privilegio de rol, se puede eliminar el privilegio de accessmgr a Creador de grupos. Como consecuencia, resulta imposible guardar o ejecutar con éxito una importación de usuarios de LDAP. Vaya al portal de gestión de acceso y seleccione Permisos de rol en las opciones. Elija la aplicación Creador de grupos y asegúrese de que haya una marca de selección en todos los recuadros de rol o una en el recuadro accessmgr.

1. Abra el panel Importar usuarios LDAP pulsando Acceso > Gestión de acceso > Importar usuarios LDAP.

   Consulte Ejemplo de configuración LDAP de Tivoli al final de este tema de ayuda para obtener información sobre cómo rellenar la información necesaria.

2. Para Nombre de host LDAP, especifique la dirección IP o nombre de host del servidor LDAP al que se accederá.
3. Para Puerto, especifique el número de puerto para conectar al servidor LDAP.
4. Seleccione el tipo de servidor LDAP del menú Tipo de servidor.
5. Marque el recuadro de selección Utilizar conexión SSL si Guardium se va a conectar al servidor LDAP utilizando una conexión SSL (Secure Socket Layer).
6. Para DN base, especifique el nodo en el árbol en el que desea empezar la búsqueda. Por ejemplo, un árbol de empresa podría empezar así: DC=encore,DC=corp,DC=root
7. Para Atributo a importar, especifique el atributo que se utilizará para importar usuarios (por ejemplo: cn). Cada atributo tiene un nombre y pertenece a una objectClass.
8. Marque el recuadro de selección Borrar miembros de grupo existentes antes de importar si desea suprimir todos los miembros de grupo existentes antes de importar.
9. Para Iniciar sesión como y Contraseña, especifique la información de cuenta de usuario que conectará al servidor de Guardium.
10. Para Ámbito de filtro de búsqueda, seleccione Un nivel para aplicar la búsqueda sólo al nivel base, o seleccione Subárbol para aplicar la búsqueda a los niveles situados debajo del nivel base.
11. Para Límite, especifique el número máximo de elementos que se devolverán. Le recomendamos que utilice este campo para probar nuevas consultas o modificaciones en las consultas existentes, de modo que no cargue un número excesivo de miembros.
12. **Opcional:** Para Filtro de búsqueda, defina un DN base, un ámbito y un filtro de búsqueda. Normalmente, las importaciones se basarán en la pertenencia a un grupo LDAP, de modo que se utilizaría la palabra clave memberOF. Por ejemplo: memberOf=CN=syyTestGroup,DC=encore,DC=corp,DC=root
13. Pulse Aplicar para guardar los valores de configuración.
    Nota: El indicador Estado de la sección Configurado-General cambiará a *Actualmente la importación de LDAP está configurada para este grupo tal como sigue* y se habilitarán los botones Modificar planificación y Ejecutar una vez ahora. Ahora puede importar desde el servidor LDAP.

Planificar Importar usuarios LDAP

Si todavía no se ha configurado la importación de LDAP, debe realizar Configurar Importar usuarios LDAP antes de realizar este procedimiento.

1. Abra el panel Importar usuarios LDAP pulsando Acceso > Gestión de acceso > Importar usuarios LDAP.

Ejecutar Importar usuarios LDAP

Cuando ejecuta la importación de usuarios de LDAP a petición, tiene la oportunidad de aceptar o rechazar cada uno de los usuarios devueltos por la consulta. Esto resulta especialmente útil para fines de pruebas. Si todavía no se ha configurado la importación de LDAP, debe realizar Configurar Importar usuarios LDAP antes de realizar este procedimiento.

1. Abra el panel Importar usuarios LDAP pulsando Acceso > Gestión de acceso > Importar usuarios LDAP.
2. Pulse Ejecutar una vez ahora. Cuando se complete la tarea, el conjunto de miembros que cumplan los criterios de selección se mostrará en el panel Resultados de consulta LDAP.
3. En el panel Resultados de consulta LDAP, marque el recuadro de selección para cada usuario que desee añadir, y pulse Importar (o Cancelar para volver sin importar ningún usuario).
4. Para ver los usuarios añadidos, abra el Explorador de usuarios pulsando Acceso > Gestión de acceso > Explorador de usuarios. Verifique que se hayan añadido las cuentas de usuario correctas.

Ejemplo de configuración LDAP de Tivoli

Tabla 1. Ejemplo de configuración LDAP de Tivoli

Nombre de host LDAP	**Valores**
Puerto	389
Tipo de servidor	Tivoli Directory
Utilizar conexión SSL	

Nombre de host LDAP	Valores
DN base	cn=sample realm,o=sample
Modalidad de importación	Elija Sustituir los atributos existentes
Inhabilitar usuario si no está en la lista de importación	
Habilitar nuevos usuarios importados	
Iniciar sesión como	cn=root
Contraseña	
Ámbito de filtro de búsqueda	Subárbol
Límite	
Atributo para importar como inicio de sesión de usuario	cn (Configurable a través del portal)
Filtro de búsqueda	
Clase de objeto para el usuario	Cumplimentar con el valor predeterminado - |(objectClass=organizationalPerson)(objectClass=inetOrgPerson)(objectClass=person)
Importar roles	Añadir una marca de selección
Atributo para importar como rol	cn
BD base de búsqueda de rol	Cumplimentar con el valor predeterminado - cn=sample realm,0=sample
Filtro de roles	
Clase de objeto para el rol	Cumplimentar con el valor predeterminado - |(objectClass=groupOfNames)(objectClass=group)(objectClass=groupOfUniqueNames)
Atributo en usuario para asociar roles	Cumplimentar con el valor predeterminado - memberOf
Atributo en rol para asociar usuarios	Cumplimentar con el valor predeterminado - member

Tema principal: Visión general de la gestión de acceso

Seguridad de datos - Jerarquía de usuarios y asociaciones de base de datos

Puede utilizar las características de seguridad de datos para crear una jerarquía de usuarios y asociar usuarios con bases de datos y servidores específicos. Las características de seguridad de datos de Guardium notifican qué usuarios han accedido a qué información, y garantizan que sólo usuarios específicos vean la información de la que son responsables.

Siga estos pasos para habilitar y utilizar las características de seguridad de datos de Guardium:

1. Habilitar seguridad de datos
2. Crear una jerarquía de usuarios
3. Crear una asociación de usuario a base de datos
4. Filtrar resultados

Cuando se utilizan características de seguridad de datos con la característica Clasificación (que descubre y clasifica datos confidenciales que se encuentran en diversas ubicaciones de la base de datos), la seguridad a nivel de datos evita que un usuario especificado vea resultados de clasificador de un origen de datos especificado (definición de origen de datos). La utilización de la seguridad a nivel de datos también evita que un usuario especificado vea resultados de tarea de auditoría cuando el tipo de tarea sea Clasificador.

Habilitar seguridad de datos

Restricción: La seguridad a nivel de datos y el panel de control de investigación no se pueden habilitar simultáneamente.

1. Inicie sesión como usuario de administración y abra el Perfil global pulsando Configuración > Perfil global.
2. Pulse Habilitar para el filtrado de seguridad a nivel de datos.

   Nota: El icono de indicador de estado para el filtrado de seguridad a nivel de datos aparecerá ahora como .

   Puede verificar que el filtrado de seguridad a nivel de datos está habilitado consultando el panel Estado de servicios (Configuración > Estado de servicios).

- Con el filtrado de seguridad a nivel de datos habilitado, inicie sesión como accessmgr para utilizar las características Jerarquía de usuarios y Asociación BD-usuario.

Crear una jerarquía de usuarios

La Jerarquía de usuarios le muestra las relaciones padre-hijo entre todos los usuarios. Las jerarquías de usuarios permiten que el padre de la relación compruebe los servidores y bases de datos especificados, pero no los hijos.

Inicie sesión como accessmgr y abra Jerarquía de usuarios pulsando Seguridad de datos > Jerarquía de usuarios.

Realice una de las opciones siguientes:

- Pulse Actualización completa de correlaciones de usuario-base de datos para ver la jerarquía completa de usuarios.
- Utilice los filtros Roles y Usuarios para ver la jerarquía de un rol o usuario específico. Pulse con el botón derecho del ratón en un nodo de la jerarquía para expandir o contraer el árbol, o para añadir un usuario a una jerarquía específica.
- Pulse Renovar la jerarquía en caché para actualizar la jerarquía.

Nota: En función de la configuración, la herencia también puede tener lugar cuando el padre hereda la seguridad a nivel de datos del hijo.

Crear una asociación de usuario a base de datos

La característica Asociación BD-usuario correlaciona usuarios con bases de datos específicas para asegurarse de que los usuarios ven sólo los datos que se les permite ver.

Inicie sesión como accessmgr y abra la Asociación BD-usuario pulsando Seguridad de datos > Asociación BD-usuario.

Realice una de las opciones siguientes:

1. Vea la correlación actual de usuarios con bases de datos pulsando Actualización completa de correlaciones de usuario-base de datos.
2. Cree una asociación BD-usuario nueva seleccionando las opciones de la lista Sugerencias de nombres de servicio y servidores y pulsando Ir.
   Nota: Una vez que la correlación se haya actualizado completamente, verá un árbol que listará todos sus servidores. Pulse cualquier nodo del árbol para ver qué usuarios están asociados actualmente con ese nodo.

   Si utiliza configuración de pila-dual, hay un nodo raíz y dos árboles de direcciones en los que podrá seleccionar. Un árbol es para la dirección IPV4, y el árbol más largo es para la dirección IPV6.

   Añada un usuario o grupo a un nodo seleccionando el nodo y pulsando Añadir usuario o Añadir grupo.

Gestión central

En un dispositivo de Gestión central, hay también un recuadro en la pantalla Asociaciones Usuario - Base de datos que permite a un usuario crear asociaciones de base de datos basadas en los datos de un nodo gestionado. Seleccione un origen remoto de sólo un recuadro que aparece para dispositivos de Gestión central. Además, hay un recuadro de selección para obtener datos de TODOS los nodos gestionados.

Filtrar resultados

La seguridad a nivel de datos en el nivel de datos observados requiere el filtrado de datos para usuarios específicos y las bases de datos específicas de las que son responsables.

El filtrado a nivel del sistema se basa en la Jerarquía de usuarios y la Asociación BD-usuario de manera que los usuarios verán sólo la información de sus bases de datos asignadas para los distintos informes, procesos de auditoría, asesoramientos de seguridad, etc. en el sistema Guardium.

Inicie sesión como usuario de administración y utilice el Perfil global para filtrar los resultados. Abra el Perfil global pulsando Configuración > Perfil global.

- Filtrado predeterminado:
  - Mostrar todo: Esta opción sólo está disponible si el usuario que ha iniciado sesión tiene definido el rol especial *datasec-exempt*, que permite que el usuario vea todos los datos como si no hubiera ninguna seguridad a nivel de datos.
  - Incluir registros indirectos: Este recuadro de selección muestra en el visor no sólo las filas pertenecientes al usuario que tiene la sesión iniciada, sino también todas las filas pertenecientes a otros usuarios de esa jerarquía.
- Escalado de proceso de auditoría: Se permite el escalado para las tareas en este tipo sólo a los usuarios que tienen el rol datasec-exempt. Los usuarios sin el rol datasec-exmpt no se muestran en la lista de escalado.

  Escalar resultados a todos los usuarios: Una marca de selección en este recuadro escala los resultados de proceso de auditoría (y versiones en PDF) a todos los usuarios, incluso si está habilitada la seguridad de datos a nivel de datos observados. El valor predeterminado está habilitado. Si el recuadro de selección está inhabilitado (no hay ninguna marca de selección en el recuadro), el escalado de proceso de auditoría sólo se permitirá a los usuarios en un nivel superior en la jerarquía de usuarios y a los usuarios con el rol datasec-exempt. Si el recuadro de selección está inhabilitado, y no hay ninguna jerarquía de usuarios, no se permite ningún escalado.

- La generación de PDF y CSV para la distribución de resultados (adjuntos a correo electrónico) utilizará los valores de perfil global predeterminados establecidos en los parámetros de Consola de administración.
- Los PDF y CSV generados desde el visor utilizarán el mismo filtrado que en la pantalla.

Nota:

Los filtros de asociación de usuario de seguridad de datos a base de datos informan sólo desde los dominios siguientes: Acceso; Excepción e Infracciones de política (así como de dominios personalizados utilizando estos dominios o tablas desde estos dominios). La asociación de usuario de seguridad de datos a base de datos no filtra ninguno de los otros dominios (informes).

Los usuarios con rol de administración podrán ver los tipos de suceso en todos los roles (la información aún se filtrará según los parámetros de seguridad a nivel de datos observados).

Si la seguridad a nivel de datos está activada, las entidades predefinidas añadidas a un dominio personalizado deben estar en el mismo dominio para que el filtro de seguridad a nivel de datos funcione correctamente.

Si la seguridad a nivel de datos está activada, y los dos asuntos de entidad predefinidos están intentando enviar datos desde dos dominios (no dominios personalizados) que utilizan una política de filtrado, el envío de los dos asuntos de entidad predefinidos no se permitirá. La seguridad a nivel de datos sólo puede aplicar un tipo de política de filtrado (por ejemplo, sólo puede haber una política dependiente de ip_servidor/nombre:servicio y otra política dependiente del origen de datos).

Tema principal: Visión general de la gestión de acceso

Cómo definir jerarquías de usuario

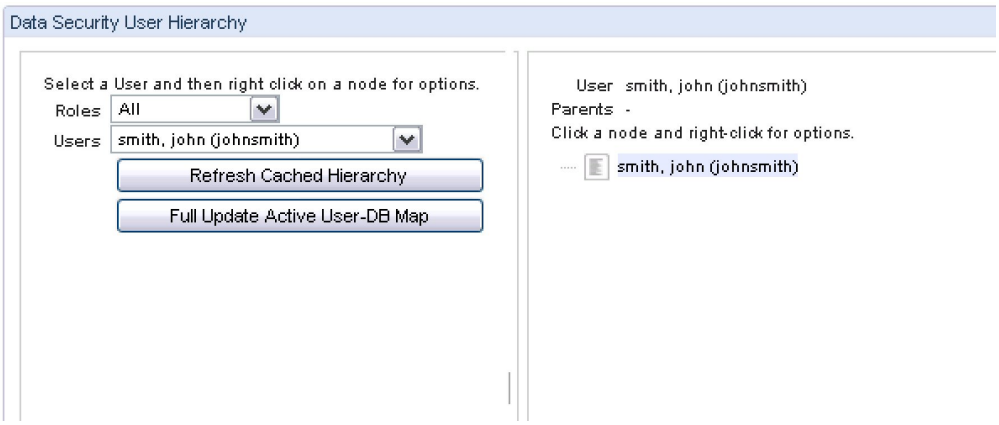
Utilice la interfaz de usuario desde una cuenta de gestor de acceso para definir fácilmente jerarquías de usuario.

Acerca de esta tarea

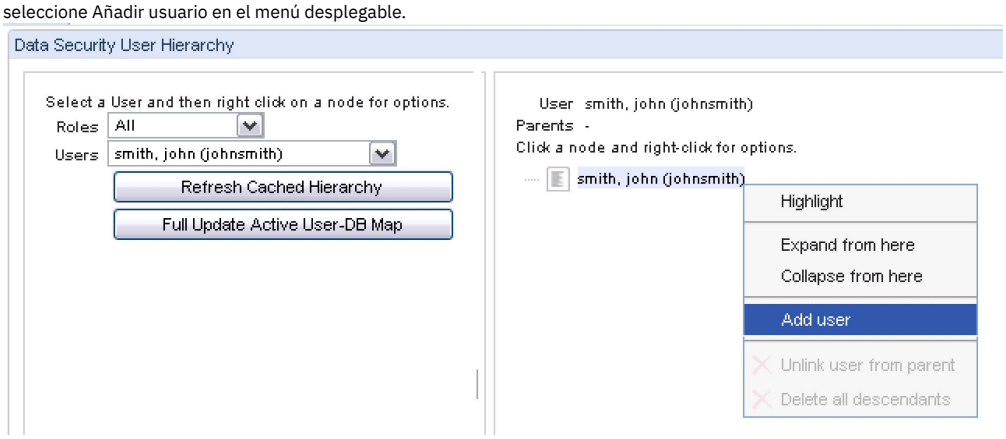
La jerarquía de usuarios de seguridad de datos representa las relaciones padre-hijo entre usuarios, y permite la creación y obligatoriedad de una seguridad a nivel de datos permitiendo que el padre de una jerarquía vea servidores o bases de datos especificados, pero no los hijos. En función de la configuración, la herencia también puede tener lugar cuando el padre hereda la seguridad a nivel de datos del hijo.

Procedimiento

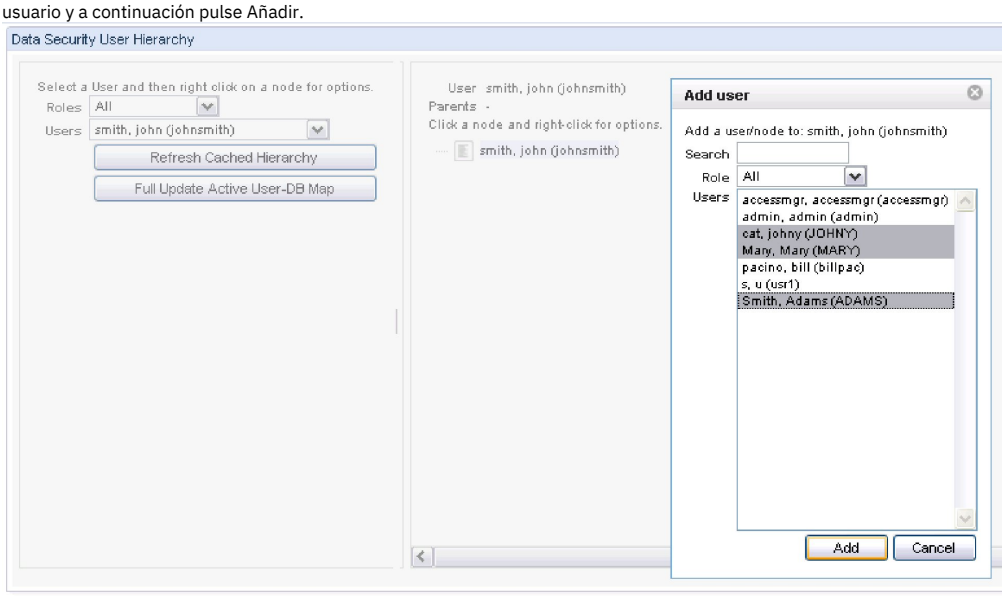
1. Inicie sesión como accessmgr y pulse Seguridad de datos > Jerarquía de usuarios.
2. Seleccione un usuario del menú desplegable Usuarios para visualizarlo en el panel Jerarquía de usuarios de seguridad de datos. Este ejemplo utiliza john smith como usuario.



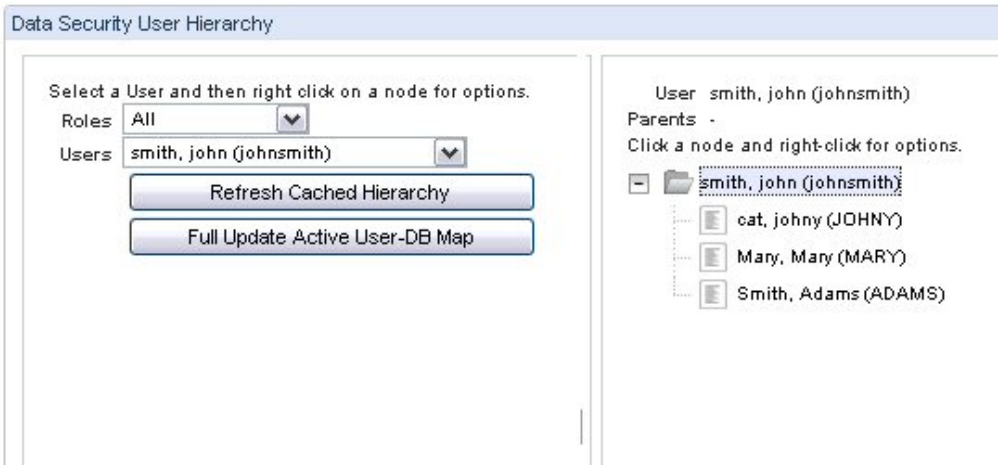
3. Para añadir un usuario a la jerarquía de john smith, pulse con el botón derecho del ratón en el usuario en el panel Jerarquía de usuarios de seguridad de datos y seleccione Añadir usuario en el menú desplegable.



4. Tras pulsar Añadir usuario en la lista desplegable, aparece el recuadro de diálogo Añadir usuario. Seleccione uno o más usuarios que desee añadir a la jerarquía del usuario y a continuación pulse Añadir.



5. Tras añadir los usuarios a la jerarquía, el panel Jerarquía de usuarios de seguridad de datos se renovará y permitirá que el usuario profundice y vea la nueva jerarquía.



6. Repita los pasos hasta que se hayan definido todos los usuarios necesarios para la jerarquía de seguridad de datos.

Tema principal: Visión general de la gestión de acceso

Inicio de sesión en la interfaz de usuario de Guardium mediante una tarjeta inteligente

El soporte de tarjetas inteligentes de Guardium satisface la regulación del gobierno de Estados Unidos con relación a que todos los proveedores deben dar soporte a la autenticación de múltiples factores (MFA) para el acceso de los usuarios. El soporte de la autenticación de tarjetas inteligentes es únicamente para el acceso a la interfaz de usuario de Guardium basada en la web.

Antes de empezar

Los detalles de los requisitos de la autenticación de múltiples factores se encuentran en la sección Identification and Authentication (Organizational Users) (IA-2) del documento Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53) del gobierno de EE.UU. El documento NIST 800-53 está disponible en el sitio web de NIST: https://www.nist.gov.

Las aplicaciones gubernamentales norteamericanas hacen referencia a las tarjetas PIV (Personal Identification and Verification Cards). Las aplicaciones de uso civil hacen referencia a las tarjetas CAC (Common Access Cards). Las tarjetas PIV y CAC tienen autoridades de certificación diferentes, pero por lo demás son iguales.

El soporte para tarjetas inteligentes de Guardium satisface el nivel de garantía PIV de ALTA confianza tal como se describe en la sección PIV Cardholder Authentication (6) del documento Personal Identity Verification (PIV) of Federal Employees and Contractors (FIPS Publication 201-2) del gobierno de EE.UU. El documento FIPS 201-2 está disponible en el sitio web de NIST: https://www.nist.gov.

Requisitos previos

El dispositivo precisa de lo siguiente:

- Acceso a la interfaz de usuario de Guardium a través de un navegador web que pueda acceder al certificado de la tarjeta inteligente
- Un lector de tarjetas inteligentes
- Una tarjeta PIV/CAC válida

Acerca de esta tarea

En esta tarea se describe como asociar correctamente la información en una tarjeta inteligente con un usuario de Guardium.

Cree los usuarios de Guardium que va a asociar a las tarjetas inteligentes. Si desea asociar usuarios existentes con tarjetas inteligentes, no necesitará crear nuevos usuarios. Para obtener más información sobre la creación de usuarios y la gestión de los accesos, consulte la Visión general de la gestión de accesos.

1. Inicie una sesión en la interfaz de usuario de Guardium como usuario administrador.
2. Vaya a Configuración > Herramientas y vistas > Portal.
3. Bajo la sección de Configuración de autenticación, seleccione la opción de Tarjeta inteligente. Si la opción de la tarjeta inteligente no está presente, verifique que se ha instalado el parche para las tarjetas inteligentes.
4. En el campo Patrón de coincidencia de expresión regular, proporcione una expresión regular (regex) que coincida con la información de usuario en la tarjeta inteligente.

Ejemplo

Creación de usuarios

La aplicación Guardium proporciona varias maneras de crear usuarios. No importa la forma en la que se crean los usuarios, y una vez su web esté configurada para utilizar tarjetas inteligentes para la autenticación, únicamente se utiliza la credencial de la tarjeta inteligente para establecer una comunicación SSL/TLS (el sitio de Guardium utiliza https).

A continuación se proporciona un ejemplo para crear un usuario de forma manual:

1. Inicie una sesión como Accessmgr en el Gestor central (CM)
2. Seleccione AccesoExplorador de usuarios.
3. Pulse Añadir.
4. Añada el nombre de usuario Test Cardholder X
5. Añada la contraseña dos veces
6. Especifique el nombre y el apellido del usuario
7. Pulse Añadir.

Ahora configurará la correlación, de forma que cuando la tarjeta inteligente esté presente, la información de la tarjeta se correlacionará de forma correcta con un usuario en el sistema.

1. Inicie una sesión como administrador desde el Gestor central (CM) o autónomamente.
2. Después de iniciar una sesión, vaya a Configuración > Herramientas y vistas > Portal.

Si ve una pantalla de menú titulada Configuración de autenticación, quiere decir que tendrá instalado el parche de soporte para las tarjetas inteligentes.

Utilice ahora una expresión regular, en el Patrón de coincidencia de expresión regular, para que coincida con la información de usuario en la tarjeta inteligente. A continuación se muestra un patrón de coincidencia para la expresión regular:

CN ?= ?(.*?), ?OU ?= ?Test Agency, ?OU ?= ?Test Department, ?O ?= ?Test Government, ?C ?= ?US

Esta expresión funciona con una tarjeta inteligente con un certificado de cliente, el certificado de cliente seleccionado para enviar al servidor web para establecer una conexión HTTPS. En la tarjeta inteligente seleccionada, se proporciona el certificado de cliente al servidor web cuando el servidor lo solicita, lo que ocurre cuando esta característica está habilitada. Un certificado de cliente tiene, por ejemplo, los siguientes detalles: Versión, Número de serie, Algoritmo de firma, Algoritmo de hash de firma, Emisor, Inicio de validez, Fin de validez o Sujeto.

En este ejemplo puede utilizar uno de los siguientes patrones. Ambos coincidirán con la correlación. El patrón 1 es más exacto. El patrón 2 depende de sus intenciones. Puede escribir su propio patrón para que coincida con sus necesidades. Necesitará trabajar con alguien más que esté familiarizado con los datos en la tarjeta inteligente para escribir patrones de correlación eficientes.

Patrón 1:

CN ?= ?(.*?), ?OU ?= ?Test Agency, ?OU ?= ?Test Department, ?O ?= ?Test Government, ?C ?= ?US

Patrón 2:

CN ?= ?(.*?)

Ambos ejemplos obtendrán el valor para el atributo CN en el sujeto del certificado que puede ver examinando los detalles del certificado en el navegador. En este caso es Test Cardholder X. Configurar este patrón de forma correcta es probablemente la parte más importante para asegurarse de que la autenticación en la tarjeta inteligente se realiza de forma satisfactoria.

Observe que la herramienta de validación de expresiones regulares actualmente disponible para otros módulos no está disponible para este propósito. (Consulte la sección de resolución de problemas, los puntos 2 y 3).

Ahora guárdela. Tenga en cuenta que todavía no ha acabado puesto que necesita habilitar la tarjeta desde la interfaz de línea de mandatos puesto que parte de la habilitación solo se puede realizar cuando el servidor está inactivo, momento en el que la interfaz gráfica de usuario no está disponible.

Antes de salir de la interfaz gráfica de usuario para la parte de la interfaz de la línea de mandatos, necesitará subir el certificado raíz de la autoridad emisora de certificados (CA) al almacén de confianza.

Suba el certificado raíz de la autoridad emisora de certificados (CA) al almacén de confianza del servidor web.

Esta parte describe cómo subir el certificado raíz de la autoridad emisora de certificados (CA) en el almacén de confianza que la interfaz gráfica de usuario utiliza. Utilice la selección Importar certificado en las pantallas Configuración de autenticación y Portal de Guardium.

Si no tiene el certificado raíz de la autoridad emisora de certificados (CA) que firmó los certificados en las tarjetas inteligentes, podrá exportar un certificado raíz desde un certificado de usuario firmado de la autoridad emisora de certificados (CA) o de una tarjeta inteligente que contenga uno.

Supondremos que ha obtenido el certificado porque el cliente se lo ha proporcionado o porque lo ha exportado desde una herramienta de gestión de certificados utilizando una tarjeta inteligente como, por ejemplo, certMgr.exe o desde herramientas como, por ejemplo, Open SSL.

El certificado raíz público de la autoridad emisora de certificados (CA) de confianza. Este es el origen más habitual de un certificado raíz en entornos que ya poseen una infraestructura de tarjetas inteligentes. Se trata de un procedimiento habitual para la autenticación y distribución de tarjetas inteligentes.

Seleccione un certificado para utilizarlo para la autenticación de tarjetas inteligentes. La cadena de firmas proporciona una lista de autoridades de creación de firmas. Habitualmente, el mejor certificado que puede seleccionar es el de la autoridad intermedia por encima del certificado del usuario.

Habilitación de la característica desde la interfaz de línea de mandatos (CLI) (solo puede realizarse en la CLI)

Para comprobar el estado, utilice el mandato de CLI,

```
show system websmartcard
```

Para activar este mandato de CLI, utilice

```
store system websmartcard on
```

Para desactivar este mandato de CLI, utilice

```
store system websmartcard off
```

Cuando la característica se desactiva, la interfaz gráfica de usuario se reinicia de forma automática con el sistema utilizando la autenticación local. Esto también es útil al desplegar por primera vez el sistema cuando la expresión regular todavía no es correcta del todo y puede apreciar errores.

Nota: A pesar de que la autenticación de tarjeta inteligente se utiliza para autenticar, el control de acceso (por ejemplo, a qué módulos tiene acceso un usuario o a qué navegación tiene el usuario) se sigue realizando de la misma manera que sin la autenticación de tarjeta inteligente.

Después de habilitar esta característica

Una vez la característica está habilitada, solo podrá acceder al sitio con una tarjeta inteligente válida (PIV, CAC, etc.).

Cuando visite la interfaz gráfica de usuario del sitio, verá una solicitud para que especifique la información de autenticación, donde se le solicitará que elija un certificado.

Los detalles anteriores son para que el administrador realice la configuración. Por lo que se refiere al usuario, si la configuración es la correcta, tan solo tendrá que utilizar la tarjeta e irá directamente al contenido del sitio.

Para un usuario con una tarjeta inteligente válida, cuando carga los sitios web, el navegador solicitará el pin de la tarjeta inteligente. Este pin permite el acceso al certificado del cliente en la tarjeta cuando es solicitado.

Después de proporcionar el pin, se visualizará la página de inicio de sesión de Guardium habitual con el campo de usuario cumplimentado de forma previa con la información de inicio de sesión extraída de la tarjeta inteligente. Observe que aquí no se utiliza una contraseña. La única cosa que se ve en el campo de usuario se extrae desde la correlación.

Por ejemplo, si los certificados son válidos y la entidad certificadora (CA) raíz del emisor de la tarjeta inteligente para Test Cardholder X está cargada en el servidor web de Guardium (consulte la sección Subir el certificado de la entidad certificadora (CA) raíz para conocer cómo hacerlo), el campo de usuario estará cumplimentado con Test Cardholder X y se le solicitará el pin de la tarjeta inteligente. Este paso es necesario para acceder al certificado de cliente en la tarjeta inteligente. El certificado del cliente permanece en la tarjeta inteligente sin que exista la posibilidad de exportarlo en un archivo. Es posible que se le solicite dos veces, y en ese caso, proporcione el pin de nuevo.

Qué hacer a continuación

Resolución de problemas y escenarios de recuperación

Después de haber habilitado la característica, cuando carga el URL de Guardium, ve una página de error.

Diagnóstico: La causa más probable es que su configuración de la expresión regular de coincidencia no sea la correcta o no tenga un certificado válido en la tarjeta.

Ha creado una expresión regular de coincidencia y no parece que esté funcionando. Puede recordar que Guardium tiene una herramienta de validación de expresiones regulares y la ha utilizado pensando que si funciona en la herramienta, es una expresión regular correcta. Desafortunadamente, a pesar de que la prueba sea satisfactoria en dicha herramienta, el patrón de expresión regular no funciona adecuadamente con configuraciones de tarjetas inteligentes.

Diagnóstico: Dicha herramienta se utiliza para encontrar si una expresión se puede encontrar dentro de un párrafo de texto. Por ello, no funcionará en este caso. Esta configuración es para extraer un elemento de texto del texto del certificado tal como se visualiza en el sujeto tal como se muestra en los detalles del certificado.

En el navegador no se le solicita seleccionar ningún certificado.

Diagnóstico: El sistema o portátil tiene la posibilidad de instalar el lector de tarjetas y la tarjeta inteligente. Una copia del certificado en la tarjeta inteligente se copia en el gestor de certificados en el sistema operativo Windows. Sin embargo, al acceder al sitio, el navegador (IE, Firefox o Chrome) no lee el certificado. En otras palabras, los tres navegadores son incapaces de leer el certificado y por lo tanto no hay una solicitud para elegir el certificado.

Esta situación se ha observador en todos los navegadores en algunos portátiles en los que se ha probado. Si este es el caso, no solo está ocurriendo con el sitio de Guardium. Otros sitios que precisan tarjetas inteligentes para funcionar también presentarán este problema. Es una situación poco habitual.

Solución: Póngase en contacto con el departamento que se encarga de gestionar sus tarjetas inteligentes.

Tema principal: Visión general de la gestión de acceso

Agregación y gestión central

La agregación le permite unir datos de varios sistemas Guardium para obtener una vista consolidada. La gestión central le permite mantener la coherencia entre sus sistemas Guardium.

- Agregación
  Recopile y fusione la información de varias unidades Guardium en un único dispositivo de agregación Guardium para facilitar una vista empresarial del uso de la base de datos.
- Gestión central
  En una configuración de gestión central, una unidad de Guardium está diseñada como Gestor central. Esta unidad se puede utilizar para supervisar y controlar otras unidades de Guardium, a las que se hace referencia como unidades gestionadas. A las unidades no gestionadas se hace referencia como unidades autónomas.
- Centro de investigación
  El centro de investigación es una extensión de los servidores de agregación. Los usuarios de investigación (una vez definidos) pueden restaurar datos y resultados de las fechas históricas seleccionadas y realizar investigación forense. Una vez que se han restaurado los días (fechas), los usuarios de investigación pueden definir y ver informes utilizando la interfaz de usuario estándar de Guardium, sólo en el ámbito de las fechas investigadas.

Agregación

Recopile y fusione la información de varias unidades Guardium en un único dispositivo de agregación Guardium para facilitar una vista empresarial del uso de la base de datos.

Proceso de agregación

- Se realiza exportando diariamente datos de los dispositivos de origen al agregador (copiando diariamente los archivos de exportación en el agregador).
- A continuación, el agregador revisa los archivos subidos, extrae cada uno de los archivos y los fusiona con el repositorio interno en el agregador.

Por ejemplo, si está ejecutando Guardium en un despliegue empresarial, puede tener varios servidores de Guardium que supervisen distintos entornos (por ejemplo, diferentes ubicaciones geográficas o unidades de negocio). Puede ser útil para recopilar todos los datos en una ubicación central para facilitar una vista empresarial del uso de la base de datos. Para ello, exporte datos de varios servidores a otro servidor que se haya configurado (durante los procedimientos de instalación iniciales) como un dispositivo de agregación. En dicho despliegue, normalmente se ejecutan todos los informes, asesoramientos, procesos de auditoría, etc., en el dispositivo de agregación para obtener una vista más amplia, no siempre una vista empresarial. Nota: El agregador no recopila datos, sino que se utiliza para presentar los datos de los recopiladores.

Los informes de agregación predefinidos se pueden encontrar en el separador Supervisor de Guardium, en Supervisor de uso de almacenamiento intermedio de empresa y en el separador Supervisor diario, Recopiladores de registro.

Tipos de dispositivo

Recopilador

Se utiliza para recopilar la actividad de la base de datos, analizarla en tiempo real y registrarla en el repositorio interno para su posterior análisis y/o reacción en tiempo real (alertas, bloqueo, etc.).
Utilice esta unidad para la captura y el análisis en tiempo real de la actividad de base de datos.

Agregador (véase las notas 1, 2)
Se utiliza para recopilar y fusionar información de varios dispositivos (recopiladores y otros agregadores) para producir una vista holística de todo el entorno y generar informes a nivel de empresa. El agregador no recopila datos por sí mismo; sólo agrega datos procedentes de varios orígenes.

Gestor central (véase las notas 1, 3, 4)
Utilice este dispositivo para gestionar y controlar varios dispositivos de Guardium.
Con el Gestor central, gestione todo el despliegue de Guardium (todos los recopiladores y agregadores) desde una única consola (la consola del Gestor central). Esto incluye la instalación de parches, actualizaciones de software y la gestión y configuración de consultas, informes, grupos, usuarios, políticas, etc.

Nota:

En muchos entornos, el Gestor central también es el Agregador. El Gestor central y el Agregador se pueden instalar en el mismo dispositivo.

Es necesario configurar el dispositivo de Guardium como agregador en el momento de la instalación de forma que sea promocionable a un gestor central.

Un Gestor central por entorno federado

Obligatoriedad de Gestor central/agregador
A partir de la versión 9.5 (v9.0 parche 500), la aplicación obligará a que un Gestor central tenga que ser un dispositivo de tipo Agregador. Esto significaría que, a partir de la versión 9.5, sólo los dispositivos de tipo Agregador serán promocionables al dispositivo de Gestor central. Los dispositivos Gestor central existentes antes de la versión 9.5 no están sujetos a este cambio.

Solución para una unidad que aparece como inactiva después de la actualización

Problema: Al actualizar el Agregador con la modalidad de búsqueda en modo CM_only o Local_only, esta unidad se muestra como inactiva en la búsqueda tras la actualización. Además, si, después de la actualización, el usuario opta por cambiar la modalidad de búsqueda a all_machines, la búsqueda no estará disponible desde el agregador.

Solución: Una vez que se haya actualizado la unidad de agregador y el usuario no desee ver que la unidad de agregador aparezca como inactiva en la ayuda contextual de la búsqueda, el usuario puede ejecutar los dos mandatos siguientes

1. grdapi enable_quick_search schedule_interval=2 schedule_units=MINUTE
2. restart network

Nota: Si el entorno estaba, y estará, en la modalidad cm_only o local_only, este paso no podrá buscar desde el agregador, simplemente hágalo para que el agregador no se muestre como inactivo.

Terminología

Tabla 1.

Término	Descripción
Dispositivo de Guardium	Sistema Guardium físico o virtual; puede ser un “recopilador” o un “agregador” (con o sin gestión central)
Unidad de Guardium	Véase Dispositivo de Guardium
Unidad de gestor	Dispositivo configurado como Gestor central
Unidad gestionada	Dispositivo gestionado por el Gestor central
Unidad autónoma	Dispositivo que no está en un entorno de Gestor central
Depurar	Para obtener el mejor rendimiento, depure todos los datos que no se necesiten. Depure para liberar espacio de disco.
Archivar	Comprima los datos de un solo día en un archivo cifrado y envíelo al agregador.

Agregación jerárquica

Guardium también da soporte a la agregación jerárquica, donde varios dispositivos de agregación se fusionan en un dispositivo de agregación central de nivel superior. Resulta útil para vistas de varios niveles. Por ejemplo, puede que necesite desplegar un dispositivo de agregación para Norteamérica agregando varias unidades, otro dispositivo de agregación para Asia agregando varias unidades, y un dispositivo de agregación global central fusionando el contenido de los dispositivos de Norteamérica y Asia en una única vista corporativa. Para consolidar los datos, todos los servidores de Guardium agregados exportan datos al dispositivo de agregación de forma planificada. El dispositivo de agregación importa los datos en una única base de datos en el dispositivo de agregación, de manera que los informes ejecutados en el dispositivo de agregación se basan en los datos consolidados de todos los servidores de Guardium agregados.

Acerca del secreto compartido del sistema

El administrador de Guardium define el secreto compartido del sistema en el panel Configuración del sistema, que se describe en la sección siguiente. El secreto compartido del sistema se utiliza para las operaciones de archivado/restauración, así como para las operaciones de gestión central y agregación. Cuando se utiliza, su valor debe ser el mismo para todas las unidades que se comunicarán. Este valor es nulo en el momento de la instalación y se puede cambiar con el tiempo.

Se utiliza el secreto compartido del sistema:

- Cuando se están estableciendo conexiones seguras entre un Gestor central y una unidad gestionada.
- Cuando una unidad agregada firma y cifra datos para la exportación al agregador.
- Cuando una unidad firma y cifra datos para el archivado.
- Cuando un agregador importa datos de una unidad agregada.
- Cuando una unidad restaura datos archivados.

En función de las prácticas de seguridad de la empresa, es posible que se le solicite que cambie el secreto compartido del sistema de vez en cuando. Puesto que el secreto compartido puede cambiar, cada sistema mantiene un archivo de claves secretas compartidos, que contiene un registro histórico de todos los secretos

compartidos definidos en ese sistema. Esto permite que un archivo exportado (o archivado) de un sistema con un secreto compartido anterior sea importado (o restaurado) por un sistema en el que ese mismo secreto compartido haya sido sustituido por uno más nuevo. Los secretos compartidos (actual e históricos) se puede exportar de un dispositivo e importar en otro mediante la CLI.

Para que la agregación funcione, el secreto compartido debe estar establecido y ser el mismo para el agregador y todos los recopiladores agregados.

Operaciones de agregación, archivado y depuración

Las operaciones de exportación planificadas envían datos desde las unidades de recopilador de Guardium a un dispositivo de agregación de Guardium. Según su propia planificación, el dispositivo de agregación ejecuta una operación de importación para completar el proceso de agregación. En cualquiera de las dos unidades, o en ambas, las operaciones de archivado y depuración están planificadas para hacer copia de seguridad de datos y depurar datos regularmente (para liberar espacio y para agilizar las operaciones de acceso en la base de datos interna). Las funciones de exportación, archivado y depuración pueden funcionar con los mismos datos, pero no en los mismos rangos de fechas. Por ejemplo, es posible que desee exportar y archivar toda la información con una antigüedad superior a un día y depurar toda la información con una antigüedad superior a un mes, con lo que siempre dejará un mes de datos en la unidad de envío.

Nota:

Al establecer la planificación de la importación en un agregador, debe planificarse para que se ejecute una vez finalizada la exportación en todos los recopiladores.

Los datos de CAS también se agregan y archivan.

Nota: La alerta de que no hay tráfico está inactiva para los servidores de agregador.

Gestión de datos en un agregador

- Exportación de datos
  - Detención de la exportación
- Importación de datos
  - Detención de la importación
- Archivado y depuración
- Detención del archivado y la depuración
- Verificación del proceso de archivado y depuración
- Informes sobre la actividad de agregación y archivado
- Restauración

Exportación de datos

Tabla 2. Exportación de datos

Tema	Descripción
Función	Comprima los datos de un solo día (normalmente de medianoche a medianoche, el día anterior) en un archivo cifrado y envíelo al agregador (o a un repositorio externo en archivador).
Planificar	Se ejecuta diariamente. Empieza inmediatamente después de la medianoche (00:10) para incluir los datos de todo el día. Se supone que tarda hasta 2 horas en completarse (promedio, según la cantidad de datos).
Proceso de alto nivel	Cree una base de datos temporal. Cargue los datos relevantes (actividad del día anterior) en la bd tmp. Actualice los ID de incremento automático en la base de datos tmp para asegurar la exclusividad. Cree un archivo de exportación comprimido cifrado de la base de datos tmp. Copie el archivo de exportación en el agregador (o en un repositorio externo en archivador).

Para exportar datos a un dispositivo de agregación, siga el procedimiento. Puede definir una configuración de exportación individual para cada unidad de Guardium.

1. Pulse Gestionar > Gestión de datos > Exportación de datos para abrir Exportación de datos.
2. Seleccione el recuadro Exportar para abrir todas las opciones adicionales para la exportación de datos.
3. En los recuadros a continuación de Exportar datos anteriores a, especifique un día de inicio para la operación de exportación como un número de días, semanas o meses anteriores al día actual, que es el día cero. Estas son medidas de calendario, por lo que si hoy es el 24 de abril, todos los datos capturados el 23 de abril tienen un día de antigüedad, independientemente de la hora a la que se realice la operación. Para archivar datos a partir de los datos de ayer, especifique el valor 1.
4. Opcionalmente, utilice los recuadros que siguen a Ignorar datos anteriores a para controlar cuántos días de datos se archivarán. El valor especificado aquí debe ser mayor que el valor de Exportar datos anteriores a, así que siempre exportará al menos dos días de datos. Si deja Ignorar datos anteriores a en blanco, exportará datos para todos los días anteriores al valor especificado en la fila Exportar datos anteriores a. Se recomienda que establezca siempre el valor Ignorar datos anteriores a; de lo contrario, exportará exactamente los mismos días una y otra vez, lo que sobrecargará la red y el agregador con datos redundantes (que se ignorarán).
5. El recuadro Exportar valores está seleccionado de forma predeterminada. En algunos casos, donde el recopilador se encuentra en un país que prohíbe la exportación de datos, y el dispositivo de agregador reside en otro país, es posible que desee deseleccionar el recuadro Exportar valores, lo que enmascararía todos los campos que contienen valores de base de datos.
6. En el recuadro Host, especifique la dirección IP o nombre de host DNS del dispositivo de agregación al que se enviarán los archivos de datos cifrados de este sistema. También existe una opción para habilitar una agregación secundaria para exportar datos a más de un agregador. Hay dos recuadros Host disponibles, el primero es necesario, mientras que el Host secundario es opcional. Esta unidad y el dispositivo de agregación al cual está enviando datos deben tener el mismo secreto compartido del sistema. Si no es así, la operación de exportación funcionará, pero el dispositivo de agregación que recibe los datos no podrá descifrar el archivo exportado y la importación fallará. Consulte Secreto compartido del sistema en Configuración del sistema para obtener más información. El secreto compartido debe ser idéntico en el sistema de exportación y en el sistema receptor. Esto es así porque, a menos que tengan el mismo secreto compartido, la configuración en el sistema de exportación no se establecerá y habrá un mensaje que indicará que un archivo de prueba no se puede enviar al sistema receptor.
7. Utilice la sección Planificación para definir una planificación para ejecutar esta operación regularmente.

8. Pulse el botón Guardar para guardar la configuración de exportación y depuración para esta unidad. Al pulsar el botón Aplicar, el sistema intenta verificar que el host de agregador especificado aceptará los datos de esta unidad. Si la operación falla, se muestra el mensaje siguiente y la configuración no se guardará: No se ha podido enviar un archivo de datos de prueba a este host. Confirme que el nombre de host o la dirección IP se hayan especificado correctamente y que el host esté en línea.
9. Pulse Ejecutar una vez ahora para ejecutar la operación una vez.

Detención de la exportación

Para detener la exportación de datos a un dispositivo de agregador:

1. Pulse Gestionar > Gestión de datos > Exportación de datos para abrir Exportación de datos.
2. Desmarque el recuadro de selección Exportar.
3. Pulse Guardar.

Nota: No es posible detener una exportación una vez que se ha pulsado el botón Ejecutar una vez ahora.

Importación de datos

Las unidades de recopilador de Guardium exportan archivos de datos cifrados a otro dispositivo de Guardium configurado como dispositivo de agregación. Los archivos de datos cifrados residen en una ubicación especial en el dispositivo de agregación hasta que el dispositivo de agregación ejecuta una operación de importación para descifrar y fusionar todos los datos en su propia base de datos interna.

Nota: Para evitar la posibilidad de importar archivos que no han llegado por completo, el dispositivo de agregación no importará archivos que hayan cambiado en los dos últimos minutos.

Tabla 3. Importación de datos

Tema	Descripción
Función	Importe y fusione los datos importados en las bases de datos internas del agregador.
Planificar	Se ejecuta diariamente. Se inicia a las 02:00 (o después de la finalización de la exportación). Se supone que puede tardar hasta 3 horas en completarse.
Proceso de alto nivel (para cada día depurado)	Construya el mandato delete para cada tabla depurada (las tablas y las condiciones de depuración definidas en AGG_TABLES). Ejecute los mandatos delete para cada una de las tablas.

Siga el procedimiento para definir la operación Importación de datos en un dispositivo de agregación. Puede definir sólo una única configuración de importación de datos en cada unidad.

1. Pulse Gestionar > Gestión de datos > Importar para abrir Importar.
2. Seleccione el recuadro Importar, que hace que aparezca un campo no modificable adicional que indica la ubicación del archivo de datos que se importará.
3. Pulse Aplicar para guardar la configuración. El botón Aplicar sólo está disponible cuando se selecciona y deselecciona el recuadro Importar datos.
4. Pulse Ejecutar una vez ahora para ejecutar la operación una vez.
5. Pulse Modificar planificación para planificar la operación para que abra el planificador de tareas general y se ejecute regularmente. Este dispositivo de agregación y todas las unidades que exportan datos a él deben tener el mismo secreto compartido del sistema. Si no es así, las operaciones de exportación funcionarán, pero el dispositivo de agregación no podrá descifrar los archivos de los datos exportados.

Detención de la importación

Para detener la importación de datos enviados desde otras unidades de Guardium:

1. Pulse Gestionar > Gestión de datos > Importar para abrir Importar.
2. Desmarque el recuadro de selección Exportar datos.
3. Pulse Aplicar para guardar la configuración. La detención de la importación no hace que otras unidades de Guardium dejen de exportar datos a este sistema. Para detener esa exportación, debe detener la operación Exportar en cada una de las unidades emisoras.

Nota: No es posible detener una importación una vez que se ha pulsado el botón EJECUTAR UNA VEZ AHORA.

Archivado y depuración

El archivado y la depuración regulares de datos es esencial para la salud del sistema Guardium. Para obtener el mejor rendimiento, recomendamos encarecidamente que archive y depure todos los datos que no se necesiten. Importe: Depure para liberar espacio de disco. Por ejemplo, si sólo necesita tres meses de datos en el dispositivo de Guardium, archive y depure todos los datos anteriores a 90 días.

El proceso de archivado y depuración libera espacio y conserva la información para utilizarla en el futuro. Debe archivar y depurar periódicamente los datos de las unidades autónomas y de las unidades de agregación. La función de archivado de Guardium crea archivos firmados y cifrados que no se pueden manipular. Los archivos de archivado se transfieren y se almacenan en sistemas externos tales como servidores de archivos o sistemas de almacenamiento.

Nota:

Si se planifica Archivar y Depurar, Depurar se ejecutará después de Archivar.

Los datos archivados en un recopilador pueden restaurarse en otro recopilador o en un servidor de agregador. La restauración en una máquina de recopilador de datos archivados en un agregador no está soportada.

Archivado de datos en el sistema agregador: el primer día del mes, todas las tablas estáticas se archivan. Todos los demás días sólo se archivarán los datos adicionales añadidos a los datos archivados. Esta metodología es la misma que la que utilizan los recopiladores. La adición de las tablas estáticas al proceso de depuración normal elimina la existencia de huérfanos, liberando espacio en disco y mejorando el rendimiento del informe.

El archivado y la exportación de tablas estáticas en un agregador incluye datos estáticos completos sólo el primer día del mes (archivado) o cuando cambia la configuración de exportación (exportación). Utilice los mandatos de CLI, store archive_table_by_date [enable | disable] o show archive_table_by_date. Otros mandatos de

CLI relevantes son store aggregator clean orphans o show aggregator clean orphans.

Planificación de tareas de gestión de datos: Cuando se crea la unidad se proporcionan horas de planificación predeterminadas, que se pueden modificar según corresponda. Las tareas de gestión de datos se deben planificar a las horas menos ocupadas, por ejemplo, durante la noche. Se deben también espaciar de forma que no se solapen (por ejemplo, el inicio de una tarea no debe solaparse con el inicio de otra tarea antes de que finalice).

Archivado de datos de agregador: Cuando se trabaja con un agregador/gestor central que realiza importaciones de datos y archivados de datos. Un valor predeterminado o común es que el archivado de datos realice un archivado de datos anteriores a un día, ignorando todos los datos con una antigüedad mayor a dos días. Si se da el caso de que el archivado de datos está planificado para ejecutarse ANTES de las importaciones de datos de otros recopiladores/agregadores, el archivado NO contendrá las importaciones destinadas al archivado de ese día. Imagine la planificación siguiente: el archivo de datos se ejecutará a las 00:30 AM; las importaciones de datos se ejecutarán a las 6:00 AM para datos anteriores a 1 día - ignorando los datos anteriores a 2 días. Cuando tenga lugar el archivado, no archivará los datos de ayer relevantes, ya que aún no se ha realizado ninguna importación de ese día. En este ejemplo, el archivado de datos se debe volver a planificar para que tenga lugar DESPUÉS de que hayan finalizado las importaciones de datos. De esta forma, el archivado contendría correctamente los datos de ayer.

Tabla 4. Archivado y depuración de datos

Tema	**Descripción**
Función de depuración	Suprima registros anteriores del dispositivo (normalmente, anteriores a 60 días) para liberar espacio y agilizar la operación de acceso a la base de datos interna. La depuración se basa en fechas (la supresión de valores de datos de días enteros), pero no suprimirá registros que aún estén “en uso” (por ejemplo: sesiones abiertas).
Planificar	La actividad de depuración predeterminada está planificada diariamente a las 5:00 AM. Recopiladores, tras la exportación/archivado. Agregador, tras la importación. Se supone que puede tardar hasta 2 horas en completarse.
Proceso de alto nivel (para cada día depurado)	La configuración de depuración la utilizan tanto el archivado de datos como la exportación de datos. Utilice el campo Depurar datos anteriores a para especificar un día de inicio para la operación de depuración como número de días, semanas o meses anteriores al día actual, que es el día cero.
Depuración predeterminada	El valor predeterminado para depuración es 60 días La actividad de depuración predeterminada está planificada diariamente a las 5:00 AM. En el caso de una instalación nueva, se instalará la planificación de depuración predeterminada según el valor y actividad predeterminados Cuando se cambia un tipo de unidad entre gestor gestionado o de nuevo a autónomo, se aplicará la planificación de depuración predeterminada. La planificación de depuración no resulta afectada durante una actualización

Es posible que sea necesario ejecutar informes o investigaciones sobre estos datos en algún momento. Por ejemplo, es posible que algunos entornos regulatorios puedan requerir que mantenga esta información durante tres, cinco o incluso siete días de tal forma que se puedan consultar durante 24 horas. La capacidad de restauración de Guardium da soporte a esta funcionalidad, que le permite restaurar datos archivados a la unidad.

Las secciones siguientes describen cómo definir y planificar el archivado y cómo restaurar desde un archivado.

Nota: Las operaciones de archivado y restauración dependen de los nombres de archivo generados durante el proceso de archivado. NO cambie los nombres de los archivos archivados.

Los archivos de datos de archivado se pueden enviar a un host SCP o FTP en la red, o a un sistema de almacenamiento EMC Centera o TSM (si se ha configurado). Puede definir una configuración de archivado individual para cada unidad. Para archivar datos en otro host de la red y, opcionalmente, depurar los datos de la unidad, siga el procedimiento.

1. Pulse Gestionar > Gestión de datos > Archivado de datos para abrir Archivado de datos.
2. Marque el recuadro de selección Archivar para exponer campos adicionales para el proceso de archivado.
3. En los recuadros que siguen a Archivar datos anteriores a, especifique un día de inicio para la operación de archivado como un número de días, semanas o meses anterior al día actual, que es cero. Estas son medidas de calendario, por lo que si hoy es el 24 de abril, todos los datos capturados el 23 de abril tienen un día de antigüedad, independientemente de la hora a la que se realice la operación. Para archivar datos a partir de los datos de ayer, especifique el valor `1`.
4. Opcionalmente, utilice los recuadros que siguen a Ignorar datos anteriores a para controlar cuántos días de datos se archivarán. Cualquier valor especificado aquí debe ser mayor que el valor del campo Archivar datos anteriores a. Si deja en blanco la fila Ignorar datos anteriores a, se archivan datos para todos los días anteriores al valor especificado en la fila Archivar datos anteriores a. Esto significa que si archiva diariamente y depura datos anteriores a 30 días, se archiva cada día de datos 30 veces (antes de que se depure el día 31). En función de las opciones de archivado configuradas para el sistema (utilizando el mandato de CLI store storage-system), puede tener opciones de EMC Centera o TSM en el panel. Si selecciona uno de los destinos de archivado, consulte el tema adecuado.
    a. Archivado y copia de seguridad de EMC Centera
    b. Archivado y copia de seguridad de TSM
5. Especifique la dirección IP o el nombre de host DNS del host para recibir los datos archivados
6. En el recuadro Directorio: Identifique el directorio en el que se van a almacenar los datos. La manera de especificar esto dependerá de si el método de transferencia de archivos es FTP o SCP. Para FTP, especifique el directorio relativo al directorio de inicio de la cuenta FTP. Para SCP, especifique el directorio como una vía de acceso absoluta.
7. En el recuadro Nombre de usuario, especifique el nombre de usuario que se utilizará para iniciar sesión en la máquina host. Este usuario debe tener permisos de escritura/ejecución para el directorio identificado en el recuadro Directorio.
8. En el recuadro Contraseña, especifique la contraseña del usuario y a continuación especifíquela de nuevo en el recuadro Vuelva a especificar la contraseña.
9. Depuración de datos
10. Marque el recuadro de selección Depurar para depurar datos, independientemente de si está archivado. Cuando este recuadro está marcado, se muestran los campos Depurar datos anteriores a. Es importante tener en cuenta que la configuración de depuración la utilizan tanto el archivado de datos como la exportación de datos. Los cambios realizados aquí se aplicarán a todas las ejecuciones de exportación de datos, y viceversa. En el caso de que la depuración esté activada y la exportación de datos y el archivado de datos se ejecuten el mismo día, la primera operación que se ejecute probablemente depurará los datos anteriores a la ejecución de la segunda operación. Por esta razón, cuando están configurados tanto la exportación de datos como el archivado de datos, la antigüedad de depuración debe ser mayor que la antigüedad de la exportación y la antigüedad del archivado.

11. Si depura datos, utilice los campos Depurar datos anteriores a para especificar un día de inicio para la operación de depuración como un número de días, semanas o meses anteriores al día actual, que es el día cero. Todos los datos del día especificado y todos los días anteriores se depurarán, excepto si se indica lo contrario. El valor especificado para la fecha de inicio de depuración debe ser mayor que el valor especificado para el valor Archivar datos anteriores. Además, si la exportación de datos está activa (consulte Exportación de datos a un dispositivo de agregación), la fecha de inicio de depuración especificada aquí debe ser mayor que el valor Exportar datos anteriores a. No hay ningún aviso cuando se depuran datos que no han sido archivados o exportados por una operación anterior. La operación de depuración no depura los datos restaurados cuya antigüedad está dentro del marco de tiempo de No depurar datos restaurados en una operación de restauración. Para obtener más información, consulte Restauración de datos archivados.
12. Utilice la sección Planificación para definir una planificación para ejecutar esta operación regularmente.
13. Pulse Guardar para verificar y guardar los cambios de configuración. Al pulsar el botón Guardar, el sistema intenta verificar el host, directorio, nombre de usuario y contraseña especificados enviando un archivo de datos de prueba a dicha ubicación.
14. Pulse Ejecutar una vez ahora para ejecutar la operación una vez.

Limpieza de huérfanos en agregadores

Cuando el agregador incluye datos restaurados, se establecerá la limpieza de huérfanos relacionada con los datos según la fecha de caducidad establecida cuando se restauraron los datos por primera vez.

Si se realizan cambios mediante mandatos de GuardAPI relacionados con la fecha de caducidad, esto no afectará a los datos restaurados de fecha que están disponibles para la limpieza de huérfanos.

Por ejemplo: el usuario restaura datos y desea mantener estos datos durante 7 días. Esto significa que la fecha de caducidad de estos datos será dentro de 7 días, a partir de hoy, y estos datos estarán disponibles para la limpieza de huérfanos después de 7 días.

Si se cambia la fecha de caducidad (se establece para mantener los datos un periodo más largo o más corto), esto no afectará a la fecha en que estos datos estarán disponibles para la limpieza de huérfanos. El cliente debe tener especialmente esto en cuenta si cambia el periodo de caducidad para que sea más largo, a fin de no perder datos; los demás datos de la máquina estarán disponibles para la limpieza de huérfanos tal como se diseñó al principio.

Archivado y copia de seguridad de EMC Centera

Para utilizar EMC Centera:

1. Pulse Gestionar > Gestión de datos > Archivado de datos para abrir Exportación de datos.
2. Pulse en Archivado de datos o Copia de seguridad del sistema en la sección Gestión de datos. Inicialmente, el botón de selección Red está seleccionado de forma predeterminada, y se muestran los parámetros de Copia de seguridad de red.
3. Seleccione el botón EMC Centera. Los parámetros de EMC Centera se mostrarán en el panel.
4. En el recuadro Retención, especifique el número de días que se retendrán los datos. El máximo es 24855 (68 años). Si desea guardarlos durante más tiempo, puede restaurar los datos posteriormente y volver a guardarlos.
5. En el recuadro Dirección de agrupación de Centera, especifique la serie de conexión de agrupación de Centera; por ejemplo:
   `10.2.3.4,10.6.7.8/var/centera/profile1_rwe.pea`
6. Pulse Subir PEA para subir un archivo PEA de Centera que se utilizará para la serie de conexión.
7. Pulse Guardar para guardar la configuración. El asistente intentará verificar la dirección de Centera abriendo una agrupación utilizando la serie de conexión especificada. Si la operación falla, se le informará y la configuración no se guardará.

Archivado y copia de seguridad de TSM

Cuando selecciona TSM como destino de archivado o copia de seguridad, la parte de TSM del panel de configuración de copia de seguridad o archivado se expande. Antes de establecer TSM como destino de archivado o copia de seguridad, el sistema Guardium debe estar registrado con el servidor TSM como un nodo de cliente. Se debe crear un archivo de opciones del sistema cliente de TSM (dsm.sys) (en el PC, por ejemplo) y subir a Guardium. En función de cómo se defina ese archivo, es posible que también deba subir un archivo dsm.opt. Para obtener ayuda para crear un archivo dsm.sys para que lo utilice Guardium, consulte al administrador de TSM de su empresa. Para subir un archivo de configuración de TSM, utilice el mandato de CLI, import tsm config.

El ciclo de vida de TSM (o cliente de Spectrum Protect) lo definen los términos del producto Spectrum Protect.

Para utilizar TSM:

1. Pulse Gestionar > Gestión de datos > Archivado de datos para abrir Archivado de datos.
2. Seleccione el botón TSM. Los parámetros de TSM se mostrarán en el panel.
3. En el recuadro Contraseña, especifique la contraseña de TSM que utiliza esta unidad de Guardium para solicitar los servicios de TSM, y vuélvala a especificar en el recuadro Vuelva a especificar la contraseña.
4. Opcionalmente, especifique un nombre de usuario que coincida con una entrada servername del archivo dsm.sys.
5. Opcionalmente, especifique un nombre Como host.
6. Pulse Guardar para guardar la configuración. Al pulsar el botón Aplicar, el sistema intenta verificar el destino de TSM enviando un archivo de prueba al servidor utilizando el mandato dsmc archive. Si la operación falla, se le informará y la configuración no se guardará.

Detención del archivado y la depuración

1. Pulse Gestionar > Gestión de datos > Archivado de datos para abrir Archivado de datos.
2. Desmarque el recuadro Archivar o Depurar.
3. Pulse Guardar.

Verificación del proceso de archivado y depuración

1. Pulse Informes > Informes operativos de Guardium > Registro de agregación/archivado para abrir el Registro de agregación/archivado.
2. Asegúrese de que la operación de archivado/depuración tiene un estado de Satisfactorio.

Informes sobre la actividad de agregación y archivado

1. Vaya a Gestionar > Informes > Gestión de datos > Registro de agregación/archivado para abrir el Registro de agregación/archivado.
2. Defina una consulta y cree un informe.

Restauración

Como se ha descrito anteriormente, los archivados se graban en un host SCP o FTP, o en un sistema de almacenamiento Centera o TSM. Para restaurar archivados, debe copiar el archivo adecuado de nuevo en el sistema Guardium en el que se deben restaurar los datos. Hay un archivo individual para cada día de datos. En función de cómo esté configurada la operación de archivado/depuración, puede que tenga varias copias de datos archivados el mismo día. Los nombres de archivo de datos de archivado y exportación tienen el mismo formato: archivo <secuencia_días>-<nombre_host.dominio>-w<run> indicación_fecha_y_hora>-d<fecha_datos>.dbdump/TAR. Para restaurar un archivo de datos archivados (y no sistema de copia de seguridad), debe utilizar la pantalla de la interfaz gráfica de usuario denominada Archivador de catálogo. Las operaciones de archivado y restauración dependen de los nombres de archivo generados durante el proceso de archivado. NO cambie los nombres de los archivos archivados. Si cambia un nombre de archivo generado, la operación de restauración no funcionará.

Por ejemplo: archivo 732423-g1.guardium.com-w20050425.040042-d2009-04-22.dbdump/TAR.

A menos que esté restaurando datos del primer archivado creado durante el mes, deberá restaurar varios días de datos. Esto se debe a que, al restaurar datos, Guardium debe tener toda la información que tenía cuando se archivaron los datos que se están restaurando. Una vez creado el archivado, parte de esa información puede haberse depurado debido a la falta de uso. Toda la información necesaria para una operación de restauración se archiva automáticamente, la primera vez que se archivan los datos cada mes. Por lo tanto, al restaurar datos, puede restaurar el primer día del mes y añadir los demás días hasta el día deseado o restaurar el día deseado y a continuación el primer día del mes siguiente

Por ejemplo, para restaurar el 28 de junio, restaure del 1 de junio al 28 de junio, o restaure el 28 de junio y el 1 de julio.

Para restaurar un archivo de datos archivados (y no sistema de copia de seguridad), debe utilizar la pantalla de la interfaz gráfica de usuario denominada Archivador de catálogo. Las operaciones de archivado y restauración dependen de los nombres de archivo generados durante el proceso de archivado. NO cambie los nombres de los archivos archivados. Si cambia un nombre de archivo generado, la operación de restauración no funcionará.

1. Pulse Gestionar > Gestión de datos > Restauración de datos para abrir Restauración de datos.
2. Especifique una fecha en el recuadro Desde, para especificar la fecha más temprana para la que desea datos.
3. Especifique una fecha en el recuadro Hasta, para especificar la fecha más tardía para la que desea datos.
4. En el recuadro Nombre de host, especifique opcionalmente el nombre del dispositivo de Guardium a partir del que se ha originado el archivado.
5. Pulse Buscar.
6. En el panel Resultados de búsqueda, marque el recuadro de selección de cada archivado que desee restaurar.
7. En el recuadro No depurar datos restaurados durante al menos, especifique el número de días que desea retener los datos restaurados en el dispositivo.
8. Pulse Restaurar.
9. Pulse Hecho cuando haya finalizado.

Resolución de problemas

Cuando escale a soporte técnico, proporcione un registro detallado desde el momento en que se produjo el problema. Vaya a Gestionar > Informes > Gestión de datos > Registro de agregación/archivado y defina un informe para el periodo de tiempo en cuestión.

Cálculo del número máximo de recopiladores por agregador

Cuando se crea un sistema Guardium desde un .ISO, se establece un valor predeterminado de 10 para el número máximo de recopiladores por agregador.

Cuando un cliente actualiza el sistema Guardium, el sistema calcula el número máximo de recopiladores utilizando la lógica siguiente:

1. Obtener el número de recopiladores de acuerdo con los datos de la tabla interna de Guardium. El valor predeterminado es 10.
2. Si el resultado del paso 1 es 0 (no se han encontrado recopiladores), el sistema establece este valor en 10.
3. Si se encuentra un número distinto de recopiladores, el sistema añadirá un 20 por ciento más al número determinado en el paso 2.
4. Por ejemplo, si el paso 1 no ha encontrado ningún recopilador, el paso 2 establecerá un valor de 10 y, a continuación, el paso 3 le añadirá 20 % y lo establecerá en 12.
5. Otro ejemplo, en el paso 1, el sistema ha encontrado cinco recopiladores que exportan a un agregador. En este caso, el valor se establece en 5. El paso 2 no es relevante puesto que el resultado es 5 y no 0. El paso 3 añadirá 20 % a 5 y establecerá este valor en 6.

Tema principal: Agregación y gestión central

Gestión central

En una configuración de gestión central, una unidad de Guardium está diseñada como Gestor central. Esta unidad se puede utilizar para supervisar y controlar otras unidades de Guardium, a las que se hace referencia como unidades gestionadas. A las unidades no gestionadas se hace referencia como unidades autónomas.

El concepto de máquina local puede hacer referencia a cualquier máquina del sistema de Gestión central. Hay algunas aplicaciones (Procesos de auditoría, Consultas, Portlets, etc.) que se pueden ejecutar en las unidades gestionadas y en el Gestor central. En ambos casos, las definiciones proceden del Gestor central y los datos proceden de la máquina local (que podría ser también el Gestor central).

Cuando se ha configurado un sistema de Gestión central, los clientes pueden utilizar el Gestor central o una unidad gestionada para crear o modificar la mayoría de las definiciones. Tenga en cuenta que la mayoría de las definiciones residen en el Gestor central, independientemente de la máquina que realmente haga la edición.

Nota:

- Mediante la función Origen remoto, un usuario en el Gestor puede ejecutar cualquier informe sobre la unidad gestionada (el usuario debe tener los privilegios de usuario correctos) y ver los datos e información de esa unidad gestionada.
- Las definiciones de plantilla de CAS se comparten entre todas las unidades de un entorno federado de la misma forma que todas las demás definiciones (informes, políticas, alertas, etc.)
- Se recomienda que un usuario ejecute informes de CAS en un gestor, especialmente los informes de CAS relacionados con configuraciones, hosts y plantillas de CAS.
- Si utiliza el Creador de dominios personalizados para crear un informe que utiliza algunas o todas las tablas remotas (tablas que se encuentran en el gestor en un entorno de Gestor central, por ejemplo, Origen de datos o Comentarios), este informe no funciona en un nodo gestionado. No se devolverán datos.

- La página Gestión central de un gestor ya no se renovará automáticamente a intervalos determinados. Esta página excederá el tiempo de espera según el tiempo de espera de la interfaz gráfica de usuario del sistema.
- Tras algún tiempo de inactividad, el sistema cerrará su sesión automáticamente y le solicitará que la vuelva a iniciar. La duración del tiempo de espera de la interfaz gráfica de usuario se puede establecer mediante el mandato de CLI show/store session timeout (el valor predeterminado es 900 segundos). Las luces de estado se renovarán cada cinco minutos cuando la sesión esté activa.
- Si un usuario intenta sincronizar o subir datos del Gestor central a nodos gestionados, todos los nodos que participen en este tipo de actividad DEBEN tener la MISMA versión de Guardium.
- Durante la transición de redundancia de la Gestión central, la sincronización de tipo de unidad puede tardar hasta cinco minutos, según cuántas unidades haya definidas en el entorno de Gestión central.

- Servicios de componentes de Guardium
  Identifique los componentes de Guardium y las ubicaciones desde las que se toman en un entorno de gestión central.
- Implementación de la gestión central
  Haga que una máquina sea un Gestor central, conecte las demás máquinas al sistema de Gestión central y registre las unidades gestionadas para que se comuniquen con el Gestor central.
- Utilización de las funciones de Gestión central
  Utilice las funciones de Gestión central para sincronizar las cuentas de usuario del portal, supervisar las unidades gestionadas e instalar políticas de seguridad en las unidades gestionadas.

Tema principal: Agregación y gestión central

Servicios de componentes de Guardium

Identifique los componentes de Guardium y las ubicaciones desde las que se toman en un entorno de gestión central.

Esta unidad se puede utilizar para supervisar y controlar otras unidades de Guardium, a las que se hace referencia como unidades gestionadas. Las unidades no gestionadas se conocen como unidades autónomas.

Tabla 1. Servicios de componentes de Guardium

Componente	Descripción
Usuarios, roles y permisos	El Gestor central controla la definición de usuarios, roles, grupos y tablas de despensa de datos para todos los sistemas gestionados. El Gestor central exporta todo el conjunto de definiciones de usuarios, roles de seguridad, grupos y tablas de despensa de datos de forma planificada o a petición. Las unidades gestionadas actualizan sus bases de datos internas cada hora. Como resultado, podría haber un retardo de hasta una hora entre la hora a la que los usuarios, roles, permisos o tablas de despensa de datos se añaden o modifican en el Gestor central y la hora a la que la unidad gestionada aplica dichas actualizaciones. Nota: Si tiene usuarios o roles de seguridad de Guardium definidos en una unidad autónoma existente que vaya a registrarse para gestión central, estas definiciones no estarán disponibles después de que se haya registrado el sistema, a menos que estos usuarios y roles de seguridad también se hayan definido en el Gestor central. No puede administrar usuarios o roles de seguridad en una unidad gestionada. Estas definiciones sólo se pueden administrar cuando se inicia sesión en el Gestor central. Cuando se desregistra una unidad para la gestión central, todos los usuarios y roles de seguridad añadidos se eliminan, dejando sólo los usuarios predeterminados (admin, accessmgr). Cuando instale un producto de complemento de Accelerator (PCI, SOX, etc.) en un entorno de Gestor central, instálelo primero en el Gestor central y a continuación en la unidad gestionada. Añada los roles y usuarios que se requieran para el acelerador en el Gestor central (y desde allí estos se sincronizarán con la unidad gestionada). La documentación de Accelerator se incluye en el módulo Accelerator. Consulte la visión general de PCI Accelerator al final de esta tabla Servicios de componentes.
Alias y grupos	Para todos los procesos que generan automáticamente alias o grupos como, por ejemplo, importación de grupos de usuarios de LDAP, generación de grupos de consultas, generación de alias de consultas, clasificador, etc. si se genera automáticamente el mismo grupo o alias en más de una máquina virtual (gestionadas por el mismo gestor), podría haber conflictos con un grupo o alias existente, que no se sustituiría.
Procesos de auditoría	Las definiciones del propio proceso de auditoría y todas sus tareas correspondientes se guardan en el Gestor central y están disponibles para todas las unidades gestionadas. Sin embargo, las planificaciones, los resultados y las listas de tareas pendientes se guardan en la máquina local. Esto significa que se pueden ejecutar las mismas tareas de proceso de auditoría en todas las unidades gestionadas, así como en el Gestor central. Sin embargo, se pueden ejecutar a distintas horas en distintas máquinas, lo que es útil si las unidades gestionadas tienen distintos periodos de carga máxima. Cada máquina tiene su propio conjunto de resultados, que se basan en los datos que ha recopilado la máquina; y cada máquina tiene su propio conjunto de listas de tareas pendientes para todos los usuarios. Las definiciones de proceso de auditoría se exportan del Gestor central a las unidades gestionadas como parte del proceso de sincronización de usuarios (consulte Sincronización de cuentas de usuario del portal). Cuando se han generado los resultados del proceso de auditoría, los resultados están disponibles para los usuarios, pero en las unidades gestionadas podría haber un retardo de hasta una hora antes de que los informes o los supervisores como por ejemplo Revisiones del proceso de auditoría pendientes se actualicen.
Consultas	Cada consulta puede obtener sólo información de base de datos de una única base de datos. Las consultas que requieren información de acceso que incluye definiciones de Gestor central y datos de unidades gestionadas no muestran datos, o bien les faltan datos.
Políticas	Las definiciones de política se guardan en el Gestor central. Sin embargo, si instala una política en una unidad gestionada, se hace una copia local y se guarda en la unidad gestionada. La razón es que la unidad gestionada es necesaria para continuar supervisando la actividad de base de datos y utilizando la política incluso cuando el gestor central no está disponible por alguna razón. Nota: La instalación de una política en un nodo gestionado no subirá esta política para el Gestor central hasta que se pulse Renovar en el Gestor central. Cuando se instalan políticas, las versiones deben coincidir entre el Gestor central y la unidad gestionada; de lo contrario, las políticas no se instalarán y se generarán errores.

Componente	Descripción
Informes	Las definiciones de informe se guardan en el Gestor central. Cuando se llama a Regenerar portlet en un Gestor central, también se envía una solicitud de gestión (https) a todas las unidades gestionadas para regenerar el portlet (con el ID de informe). Cuando se llama a Regenerar en una unidad gestionada, si se llama desde la pantalla (no la solicitud de gestión), se debe enviar una solicitud de gestión al gestor para renovar el portlet (este se enviaría también a todas las unidades). Hay un mecanismo persistente para solicitudes de gestión para el caso de que una unidad está inactiva. Consulte las secciones de este tema sobre el registro y la instalación de política. En el Gestor central, los informes y procesos de auditoría pueden utilizar datos de una unidad gestionada pero no agregadores gestionados. La unidad gestionada se selecciona como parámetro de tiempo de ejecución, se denomina origen de datos remoto y se presenta como una lista de selección desplegable filtrada que contiene sólo unidades gestionadas. Cuando un proceso de auditoría hace referencia a un origen de datos remoto, ese proceso de auditoría se puede ejecutar sólo desde el Gestor central, de forma que no aparecerá en una lista de procesos de auditoría que se muestre en una unidad gestionada. Nota: Determinados informes, en un Gestor central, de dominio Uso de almacenamiento intermedio de sniffer (por ejemplo, Velocidad de solicitudes, Uso de CPU, Supervisor de uso de almacenamiento intermedio) NO mostrarán datos. Los informes estarán vacíos.
Asesoramiento de seguridad	Como el proceso de auditoría, la definición del propio Asesoramiento de seguridad se guarda en el Gestor central. Sin embargo, los resultados se guardan en la máquina local. Esto significa que el mismo Asesoramiento de seguridad se puede ejecutar en todas las unidades gestionadas, así como en el Gestor central.
Líneas base	Las líneas base siempre se guardan en el Gestor central. Sin embargo, las líneas base se GENERAN utilizando los datos registrados que son locales en la máquina en la que se generan. Por lo tanto, si desea incluir construcciones de todas las unidades gestionadas, debe volver a generar la línea base en TODAS las unidades gestionadas y fusionar los nuevos resultados en la línea base existente. Atención: El Creador de línea base y su funcionalidad está en desuso desde Guardium V10.1.4.
Comentarios	Los comentarios pueden guardarse en la máquina local o en el Gestor central, en función de a qué esté asociado el comentario. Si el comentario está asociado con una definición que reside en el Gestor central, también se guarda en el Gestor central. Si el comentario está asociado con un resultado en la máquina local, O algo específico de una unidad gestionada (como un motor de inspección), el comentario también se guarda en la máquina local.
Planificaciones	Las planificaciones siempre se guardan en la máquina local, incluso cuando la definición se guarda en el Gestor central.
Tareas que no son de Gestor central	Cuando un servidor está configurado como un Gestor central, se debe tener en cuenta las tareas que no se pueden realizar en esa unidad, pero que se deben realizar en otras unidades (que no sean Gestor central). Los motores de inspección no se pueden definir en el Gestor central y sólo se pueden crear en las unidades gestionadas. Sin embargo, los motores de inspección se pueden ver desde el Gestor central.
Consideraciones sobre la actualización	Se recomienda que tenga su Gestor central y unidades gestionadas en la misma versión. Primero debe actualizarse el Gestor central y a continuación las unidades gestionadas. Si se tiene un gestor con una versión distinta que sus unidades gestionadas, esto debe ser temporal, y se recomienda encarecidamente que actualice todas las unidades gestionadas a la misma versión que el gestor. Ejecute la sincronización (renovación) en todos los nodos gestionados después de actualizar, para que estos nodos gestionados reconozcan la versión de software adecuado en la que están.
PCI Accelerator for Compliance	PCI Data Security Standard consta de doce requisitos básicos. La mayor parte de los requisitos se centran en proteger la infraestructura física (por ejemplo, Requisito 1: Instalar y mantener una configuración de cortafuegos para proteger los datos) o en implementar prácticas recomendadas en procedimientos (por ejemplo, Requisito 5: Usar y actualizar regularmente el software antivirus). Sin embargo, se pone un énfasis adicional en la supervisión y el seguimiento en tiempo real del acceso a los datos de los titulares y el asesoramiento continuo del estado de salud de la seguridad de base de datos (por ejemplo, Requisito 10: Rastrear y supervisar los accesos a los recursos de red y a los datos de los titulares de las tarjetas). PCI Accelerator for Database Compliance de Guardium está personalizado para simplificar los procesos organizativos necesarios para dar soporte a estos mandatos de supervisión y seguimiento y para permitir la seguridad de los datos de titulares de tarjetas. Las plantillas de informes de Accelerator se pueden personalizar para reflejar directamente requisitos organizativos y normativos específicos. Puede acceder a estas plantillas mediante los separadores proporcionados: • Visión general de PCI Data Security Standard • Planificación y organización • PCI Req. 10: Rastrear y supervisar acceso • PCI Req. 11: Probar y validar regularmente • Supervisión de infracciones de políticas de PCI Otras herramientas de la familia de soluciones de Guardium disponibles para ayudar a cumplir las regulaciones son las siguientes: • Tarjeta de informe de cumplimiento PCI: Vista detallada de la salud de la seguridad de acceso de bases de datos de titulares de tarjetas que se utiliza para automatizar los procesos de cumplimiento con instantáneas continuas en tiempo real personalizadas para pruebas, pesos y asesoramientos definidos por el usuario. La tarjeta de informe se puede generar mediante el asesoramiento de seguridad. • Seguimiento de auditoría completo: Generación no intrusiva de un seguimiento de auditoría completo para uso de datos y modificaciones que requiere el cumplimiento normativo. • Planificación automatizada: Planificación automatizada de flujos de trabajo de PCI, tareas de auditoría y diseminación de información a las partes responsables en la organización.

La tabla siguiente puede ayudarle a identificar qué componentes se toman de qué ubicación en un entorno de gestión central.

Tabla 2. Componentes y ubicación en un entorno de Gestor central

Gestor central	Unidad gestionada
Usuarios	Configuración del sistema
Roles de seguridad	Motores de inspección

Gestor central	Unidad gestionada
Permisos del rol de aplicación	Alertador (configuración)
Consultas	Detección de anomalías
Informes	Inferencia de sesiones
Periodos de tiempo	Creación de alias IP-Nombre de host
Alertas	Copia de seguridad del sistema
Asesoramientos de seguridad	Agregación/archivado
Definiciones de procesos de auditoría	Alertas personalizadas
Conjuntos de privacidad	Procedimientos de ID personalizados
Líneas base Atención: El Creador de línea base y su funcionalidad está en desuso desde Guardium V10.1.4.	Salida csv exportada
Políticas	Planificaciones
Grupos	Configuraciones de descubrimiento automático de BD
Alias	Resultados del proceso de auditoría

Los usuarios, roles de seguridad, definiciones de proceso de auditoría y grupos se exportan desde el Gestor central a todas las unidades gestionadas de una forma planificada, tal como se describe posteriormente.

Desde el Gestor central, el administrador puede:

- Registrar unidades de Guardium para la gestión
- Supervisar unidades gestionadas (disponibilidad de usuario, estado del motor de inspección, etc.)
- Ver archivos de registro del sistema (syslogs) de las unidades gestionadas
- Ver informes que utilizan datos en unidades gestionadas
- Ver estadísticas principales para unidades gestionadas
- Instalar políticas de seguridad de Guardium en las unidades gestionadas
- Reiniciar las unidades gestionadas
- Gestionar motores de inspección de Guardium en las unidades gestionadas
- Mantener todo el conjunto de usuarios, roles de seguridad, grupos y permisos del rol de aplicación utilizados en todos los sistemas gestionados
- Distribuir parches
- Distribuir archivos JAR subidos
- Distribuir valores de copia de seguridad de parches
- Distribuir configuración de autenticación
- Distribuir configuraciones

Nota: Los permisos del rol de aplicación también los puede cambiar el administrador desde cualquier unidad gestionada. Cuando esto sucede, los permisos se cambian para todas las unidades gestionadas.
Tema principal: Gestión central

Implementación de la gestión central

Haga que una máquina sea un Gestor central, conecte las demás máquinas al sistema de Gestión central y registre las unidades gestionadas para que se comuniquen con el Gestor central.

- Implementación de la gestión central en una instalación nueva
- Implementación de la Gestión central en una instalación existente
- Si la unidad de gestión central no está disponible

- Implementación de la gestión central en una instalación nueva
  Haga que una máquina sea el Gestor central, utilice el mismo secreto compartido, registre las unidades y agrupe las unidades gestionadas.
- Implementación de la Gestión central en una instalación existente
  Implemente la Gestión central en un entorno de Guardium existente y migre un recopilador de CAS con instancias activas que se gestionarán.

Tema principal: Gestión central

Implementación de la gestión central en una instalación nueva

Haga que una máquina sea el Gestor central, utilice el mismo secreto compartido, registre las unidades y agrupe las unidades gestionadas.

Hacer que una máquina sea el Gestor central

Lo primero es hacer que una sola máquina sea un Gestor central. Seleccione una máquina. A continuación, realice los pasos siguientes.

1. Inicie sesión en la CLI de la máquina que desea convertir en el Gestor central.
2. Especifique store unit type manager. Este paso hace que la máquina sea un Gestor central, pero aún no gestiona.

Utilizar el mismo secreto compartido

Cuando tenga un Gestor central, deberá conectar las otras máquinas al sistema de Gestión central. Por motivos de seguridad, es un requisito que las comunicaciones entre las máquinas se cifren utilizando el mismo secreto compartido. Para realizar este paso, realice los siguientes elementos de acción.

1. Pulse Configuración > Herramientas y vistas > Sistema para abrir Sistema.
2. Establezca el secreto compartido en la misma serie en todos los sistemas.

- Registro de unidades
  Registre las unidades gestionadas para la comunicación con el Gestor central.
- Desregistro de una unidad gestionada
  Cuando desregistre una unidad, desregistre siempre desde el Gestor central. Este método es la única forma de que el Gestor Central disminuya su recuento de unidades gestionadas.
- Sincronización de cuentas de usuario del portal
  Gestione la sincronización de usuarios del portal mediante el Gestor central.

Tema principal: Implementación de la gestión central

Registro de unidades

Registre las unidades gestionadas para la comunicación con el Gestor central.

Puede registrar unidades de Guardium para la gestión central desde el Gestor central o desde la propia unidad. Independientemente de cómo se haya realizado el registro, el Gestor central y todas las unidades gestionadas deben tener el mismo secreto compartido del sistema. Si la unidad que se va a gestionar ya está registrada para la gestión central con otro gestor, desregistre la unidad de ese gestor central antes de registrarla con el nuevo gestor. Asegúrese de comprender exactamente qué le sucede a esa unidad cuando se registra y desregistra para la gestión central.

Nota: Si el usuario que ha iniciado la sesión en una unidad gestionada no existe en el Gestor central, la sesión queda invalidada. Permanece invalidada hasta que la unidad se registra con un Gestor central.

Qué sucede durante el registro

Durante el registro se realizan las acciones siguientes.

- El tipo de unidad se establece en gestionada y se almacena la IP del gestor.
- Se aplica la clave de producto de gestor. (La clave de licencia no se propaga con ping o sincronización de usuario. Se envía durante el registro o cuando se renueva el sistema).
- Toda la planificación de trabajos se restablece al valor predeterminado.
- Se eliminan todos los archivos psml (personalizaciones de la interfaz gráfica de usuario del portal).
- Se eliminan todos los usuarios y roles locales.
- Se restablece la lista de alertas de umbral que no se evaluará.
- Se cargan los roles y permisos de usuarios desde el gestor.
- Se suben las clases personalizadas, los JAR subidos por el usuario y el almacén de confianza LDAP desde el gestor.
- Se habilita la conexión de base de datos de gestionada a gestor.
- Se habilita la conexión de base de datos de gestor a gestionada.
- Se inicia el escucha de CAS, si es necesario.

Tras el registro, todas las definiciones de informes, consultas, grupos, políticas, auditorías y más se recuperan del Gestor central.

Si el estado de la unidad registrada continúa siendo fuera de línea

Si sabe que la unidad que está registrada está en línea y es accesible desde el Gestor central, pero su estado permanece fuera de línea, realice los pasos siguientes.

- Verifique que la unidad que se va a gestionar está en línea, accesible y operativa utilizando una ventana de navegador para iniciar sesión en el sistema Guardium en dicha unidad.
- Pulse Renovar para la unidad.
- Compruebe que haya especificado la dirección IP correcta para esa unidad.
- Compruebe que la unidad tenga el mismo secreto compartido que el Gestor central.

Nota: Si el registro de una unidad está fuera de línea, la solicitud de registro persiste. Se reenvía a la IP/el puerto especificado con un intervalo establecido, hasta que la unidad se registra. Una solicitud de registro que no se realice correctamente caduca al cabo de siete días.

Registro desde una unidad gestionada

En una unidad gestionada, puede utilizar la interfaz gráfica de usuario para registrar la unidad con el Gestor central. De lo contrario, puede utilizar el mandato register de CLI tal como se describe en la sección Registro de una unidad gestionada con la CLI.

1. Pulse Configuración > Gestión central > Registro y equilibrio de carga para abrir Registro de gestión central.
2. Para IP de host, especifique la dirección IP del Gestor central.
3. Para Puerto, especifique el puerto https del Gestor central (normalmente 8443).
4. Pulse Registrar.

Después de registrarse en la unidad gestionada, esta inicia la comunicación con el Gestor central y no es necesario hacer nada más.

Nota: La unidad de gestión central debe estar en línea y accesible para esta unidad cuando haga el registro para la gestión central. Por el contrario, si registra unidades para la gestión desde la unidad de gestión central, puede registrar unidades que no estén accesibles en ese momento.

Registro de una unidad gestionada con la CLI

1. En la unidad gestionada, inicie sesión en la CLI.
2. Especifique `register management <IP del gestor> <Puerto del gestor>`

Después de registrarse en la unidad gestionada, esta inicia la comunicación con el Gestor central y no es necesario hacer nada más.

Registro de unidades desde el Gestor central

Puede registrar unidades que no estén accesibles en ese momento.

1. Vaya a Gestionar > Gestión central > Gestión central para abrir Gestión central.
2. Pulse Registrar nuevo. Se abre la página Registro de unidades.
3. Especifique la IP y el puerto de la unidad y pulse Guardar. La página Gestión central se renueva con la nueva unidad.

Tema principal: Implementación de la gestión central en una instalación nueva

Desregistro de una unidad gestionada

Cuando desregistre una unidad, desregistre siempre desde el Gestor central. Este método es la única forma de que el Gestor Central disminuya su recuento de unidades gestionadas.

El desregistro de la unidad gestionada NO desregistra la unidad del Gestor central. El Gestor central aún cuenta esa unidad como unidad gestionada para fines de licencias y la trata como gestionada. Podría ser que no permitiera que otra unidad se registrara con el Gestor central. La función de desregistrar en la unidad gestionada se incluye SÓLO para uso de emergencia. Si un gestor ya no está en servicio, debe desregistrar la unidad antes de poder registrarla en otro gestor.

Si desregistra una unidad de la unidad gestionada, aún se muestra en la pantalla del Gestor central. Si pulsa Renovar para esa unidad, la volverá a registrar. Si pulsa cualquier otra operación para esa unidad, recibirá un mensaje de que la unidad ya no está gestionada y la eliminará del gestor.

En una unidad gestionada, puede utilizar la interfaz gráfica de usuario para desregistrar la unidad con el Gestor central. Además, puede utilizar el mandato unregister de CLI tal como se describe en Desregistro de una unidad gestionada con la CLI.

1. Inicie sesión como usuario de administración en la interfaz de usuario de Guardium de la unidad que se va a gestionar.
2. Pulse Establecer > Gestión central > Registro y equilibrio de carga para abrir Registro de gestión central.
3. Pulse Desregistrar.

Qué sucede durante el desregistro

Durante el desregistro se realizan las acciones siguientes.

- El tipo de unidad se establece en autónoma.
- Se borra la IP del gestor.
- Se borra la clave del producto (la licencia es nula hasta que se cargue manualmente una licencia o registro en un nuevo gestor).
- Se restablece la lista de alertas de umbral que no se evaluará.
- Toda la planificación de trabajos se restablece al valor predeterminado.
- Se eliminan los archivos Psml.
- Se eliminan todos los usuarios excepto los usuarios predeterminados (admin, accessmgr).
- Se inhabilita la conexión de base de datos de gestionada a gestor.
- Se reinicia la interfaz gráfica de usuario.

Después del desregistro, se recuperan todas las definiciones de informes, consultas, grupos, políticas, auditorías y más de la base de datos local, las definiciones almacenadas en el Gestor central dejan de ser accesibles.

Si no está seguro sobre cómo realizar la verificación, póngase en contacto con el soporte de Guardium antes de desregistrar la unidad.

Desregistro de una unidad desde el Gestor central

1. Inicie sesión, como usuario de administración, en el Gestor central.
2. Pulse Gestionar > Gestión central > Gestión central para abrir Registro.
3. Marque la casilla de selección de la unidad gestionada que desea desregistrar.
4. Pulse Desregistrar.

Si se desregistra una unidad gestionada desde la pantalla del Gestor central, se elimina de la lista de unidades gestionadas y se establece como unidad autónoma.

Nota: La clave de producto de la unidad se elimina y, a menos que la unidad se registre en otro gestor, la clave del producto se coloca manualmente.

Desregistro de una unidad gestionada

En una unidad gestionada, puede utilizar la interfaz de usuario para desregistrar la unidad con el Gestor central. Además, puede utilizar el mandato unregister de CLI tal como se describe en Desregistro de una unidad gestionada con la CLI.

1. Inicie sesión como usuario de administración en la unidad gestionada.
2. Pulse Configuración > Gestión central > Registro y equilibrio de carga para abrir Registro.
3. Pulse Desregistrar.

Para desregistrar una unidad gestionada mediante la CLI, realice los pasos siguientes.

1. En la unidad gestionada, inicie sesión en la CLI.
2. Especifique `unregister management`.

Cuando se ha desregistrado la unidad gestionada, esta interrumpe la comunicación con el Gestor central y no es necesario hacer nada más.

Tema principal: Implementación de la gestión central en una instalación nueva

Sincronización de cuentas de usuario del portal

Gestione la sincronización de usuarios del portal mediante el Gestor central.

Acerca de esta tarea

Como se ha mencionado anteriormente, el Gestor central controla la definición de usuarios, los roles de seguridad, los grupos y las tablas de despensa de datos para todas las unidades gestionadas. El Gestor central hace una copia cifrada y firmada de su completo conjunto de roles de seguridad y usuarios. Además, el Gestor central transmite esa información a todas las unidades gestionadas. Adicionalmente, también se copia algunas otras definiciones para el proceso local (grupos y miembros de grupo, procesos de auditoría, alias y otros) que se requieren. A continuación, las unidades gestionadas actualizan sus bases de datos internas cada hora. Este proceso significa que podría haber un retardo de hasta una hora antes de utilizar estos roles o tablas de despensa de datos.

Se produce un ciclo de sincronización de usuarios completo al realizar el registro o pulsar Renovar desde la pantalla Gestión central. En ambos casos, la información sincronizada se envía desde el gestor y se carga inmediatamente en las unidades gestionadas.

Nota: Tenga cuidado al establecer la planificación para que no interfiera con otros trabajos planificados como Importar, que es posible que no se puedan iniciar.

Procedimiento

Pulse Gestionar > Gestión central > Sincronización de usuarios del portal para gestionar la sincronización de usuarios del portal.

a. Pulse Modificar planificación para cambiar la planificación de la tarea de sincronización de usuarios mediante el planificador de tareas estándar.
b. Si la tarea se planifica activamente, pulse Poner en pausa para detener ejecuciones planificadas adicionales.
c. Si la tarea está en pausa, pulse Reanudar para empezar a ejecutar la tarea de nuevo (de acuerdo con la planificación definida).
d. Pulse Ejecutar una vez ahora para ejecutar la tarea de sincronización inmediatamente.
   Nota: La tarea que está planificada o con Ejecutar una vez ahora hace referencia a la recopilación de datos y su transmisión a las unidades gestionadas solamente. Es posible que las unidades gestionadas no utilicen esos datos para actualizar sus tablas de usuario hasta 1 hora después de recibirlos.

Tema principal: Implementación de la gestión central en una instalación nueva

Implementación de la Gestión central en una instalación existente

Implemente la Gestión central en un entorno de Guardium existente y migre un recopilador de CAS con instancias activas que se gestionarán.

En un entorno de Guardium existente, consulte el procedimiento descrito para desarrollar un plan para implementar la gestión central. Si está convirtiendo una unidad de Guardium existente en un Gestor central, tenga en cuenta que un Gestor central no puede supervisar el tráfico de la red. Por ejemplo, los motores de inspección no se pueden definir en un Gestor central.

1. Seleccione un secreto compartido del sistema para que lo utilice el Gestor central y todas las unidades gestionadas. Para obtener más información, consulte el secreto compartido del sistema en Configuración del sistema.
2. Instale la unidad de Gestor central o designe uno de los sistemas existentes como Gestor central. En cualquier caso, utilice el mandato store unit type para establecer el atributo manager para el Gestor central.
3. Las definiciones de la unidad autónoma que desea tener disponibles en el entorno de gestión central deben exportarse antes de que la unidad autónoma se registre para la gestión. Posteriormente, estas definiciones se importan en el Gestor central. ANTES de exportar o importar cualquier definición, siga el procedimiento que se describe para cada unidad autónoma que va a convertirse en una unidad gestionada. Lea la información introductoria en Definiciones de exportación/importación.
   - Decida las definiciones del sistema autónomo que desea que estén disponibles después de que el sistema pase a ser una unidad gestionada. Ignore todos los componentes del sistema autónomo que no desee que estén disponibles.
   - Compare los grupos y roles de seguridad definidos en la unidad autónoma con los que están definidos en el Gestor central. En la gestión central, se aplica una única versión de estas definiciones a todas las unidades. Si existe un rol de seguridad con el mismo nombre en ambos sistemas y se utiliza para distintos fines, añada un nuevo rol en el Gestor central y asigne el nuevo rol a las definiciones adecuadas después de que se hayan importado.
   - Si existe el mismo nombre de grupo en la unidad autónoma y en el Gestor central pero tiene miembros diferentes, cree un nuevo grupo duplicado en el sistema autónomo, teniendo cuidado de seleccionar un nombre de grupo que no exista en el Gestor central. En todas las definiciones que se van a exportar, cambie las referencias de nombres de grupo anteriores por referencias de nombre de grupo nuevas.
   - Todos los roles de seguridad asignados a todas las definiciones que se exportan desde el sistema autónomo. Cuando se importan las definiciones, se importan SIN roles, por lo que debe añadirlos manualmente.
   - Compruebe los permisos de rol de aplicación en cada sistema. Si algún rol de seguridad asignado a una aplicación en la unidad autónoma no se encuentra en el Gestor central, añádalos al Gestor central.
   - Exporte todas las definiciones desde el sistema autónomo que desea que estén disponibles después de que el sistema pase a ser una unidad gestionada. (Consulte Exportar/Importar definiciones) No exporte usuarios o roles de seguridad. Si no está seguro de una definición, expórtela en una operación de exportación aparte de manera que pueda decidir en el futuro si desea importar esa definición al Gestor central. Después de registrarse para la gestión central, ninguna de las definiciones anteriores de la unidad autónoma está disponible.
   - En la unidad autónoma, cree resultados de proceso de auditoría en versiones en PDF y almacénelos en una ubicación adecuada. Bajo la gestión central, sólo están disponibles los resultados de auditoría generados bajo la gestión central.
   - En la unidad autónoma, indique a todos los usuarios que eliminen todos los portlets que contenga informe personalizado, y que no creen nuevos informes hasta que se haya completado la conversión a gestión central.
   - En el Gestor central, añada manualmente todos los usuarios desde la unidad autónoma.
   - En la unidad autónoma, suprima todas las definiciones de usuario excepto el usuario de administración (que no se puede suprimir).
   - Registre la unidad autónoma para la gestión central. Consulte Registro de unidades para la gestión central.
   - En el Gestor central, importe todas las definiciones exportadas desde el sistema autónomo. Asegúrese de que las referencias a los elementos incluidos (receptores en notificaciones de alerta, por ejemplo) sean correctas. Vuelva a asignar los roles de seguridad, si es necesario, a todas las definiciones importadas.
   - Importe a los usuarios de la unidad gestionada de que deben utilizar la aplicación Creador de informes para generar portlets para cualquier informe personalizado que deseen visualizar en sus diseños.

Migración de un recopilador de CAS autónomo a gestionado

Utilice los pasos siguientes cuando migre un recopilador de CAS con instancias activas a gestionado.

1. Exporte las definiciones de host de CAS desde el recopilador autónomo.
2. Gestione el recopilador autónomo.
3. Reinicie el host de CAS desde la GUI del ahora recopilador gestionado.
4. Importe la definición de host de CAS al gestor.
5. Reinicie de nuevo el host de CAS desde la interfaz gráfica de usuario del recopilador gestionado.

Cuando se han realizado estos pasos, el recopilador de CAS tiene las mismas instancias y supervisa los mismos archivos que cuando era autónomo.

Nota: Los datos de CAS recopilados cuando era autónomo se suprimen. No se recopilan datos de CAS a menos que un archivo cambie.
Tema principal: Implementación de la gestión central

Utilización de las funciones de Gestión central

Utilice las funciones de Gestión central para sincronizar las cuentas de usuario del portal, supervisar las unidades gestionadas e instalar políticas de seguridad en las unidades gestionadas.

- Vistas de salud de despliegue
  Las vistas de salud de despliegue recopilan y muestran información sobre todo el entorno de Guardium en potentes vistas gráficas de fácil utilización.
- Inventario de despliegue
  La vista de inventario proporciona una vista centralizada de todos los servidores de base de datos y de los clientes GIM o S-TAP instalados.
- Vista Despliegue de recursos
  La vista Despliegue de recursos proporciona una vista centralizada de todos los servidores de base de datos y sus recopiladores, agregadores y gestores centrales asociados.
- Creación de grupos de unidades gestionadas
  Organice las unidades gestionadas en grupos y, a continuación, realice acciones en estos grupos.
- Supervisión de unidades gestionadas
  Supervise las unidades gestionadas mediante la gestión central.
- Instalación de políticas de seguridad en unidades gestionadas
  Instale una política de seguridad en una unidad gestionada.
- Gestión central de parches
  Proporciona visibilidad y control sobre la instalación, el estado, y el historial de parches.
- Utilización de perfiles de configuración
  Los perfiles de configuración le permiten definir valores de configuración y planificación desde un gestor central y distribuir dichos valores a grupos de unidades gestionadas sin alterar la configuración del propio gestor central.
- Distribuir configuración
  Las configuraciones y sus planificaciones se pueden distribuir, ya sea todas o individualmente, entre el Gestor central y las unidades gestionadas.
- Distribuir configuración de autenticación
  En lugar de configurar la autenticación en cada dispositivo individualmente, la autenticación de gestión central (Configurar autenticación) se puede configurar una sola vez en el gestor central y, a continuación, distribuir a todas las unidades gestionadas. De esta forma, la información se especifica una única vez y se aplica a algunas o a todas las unidades; algunas de las unidades pueden tener un tipo distinto de autenticación.
- Redundancia de la Gestión central
  Utilice Redundancia de la Gestión central o Gestor central secundario para configurar un Gestor central secundario o de copia de seguridad en caso de que el Gestor central primario deje de estar disponible.

Tema principal: Gestión central

Vistas de salud de despliegue

Las vistas de salud de despliegue recopilan y muestran información sobre todo el entorno de Guardium en potentes vistas gráficas de fácil utilización.

Las vistas de salud de despliegue le ayudan a investigar las tendencias de utilización del sistema y a identificar rápidamente los sistemas inactivos o que fallan. Estas vistas reducen los tiempos de reacción y el riesgo de problemas en el despliegue de Guardium. Las vistas de salud de despliegue están diseñadas para funcionar conjuntamente consolidando distintas fuentes de información en vistas exclusivas pero relacionadas.

Vistas de tabla y topología de salud de despliegue

Las vistas de tabla y topología de salud de despliegue muestran las relaciones de flujo de datos entre los sistemas del entorno. Estas vistas facilitan la identificación de los sistemas problemáticos y la investigación de los problemas subyacentes.

Para acceder a la vista de topología, vaya a Gestionar > Vista de sistema > Topología de salud de despliegue. Para acceder a la vista de tabla, vaya a Gestionar > Vista de sistema > Tabla de salud de despliegue.

Panel de control de salud de despliegue

El panel de control de salud de despliegue proporciona un resumen rápido de los problemas encontrados en un despliegue de Guardium. El panel de control resulta especialmente útil para identificar patrones y tendencias en los datos de salud antes de investigar sistemas individuales en los que se identifican problemas.

Para acceder al panel de control, vaya a Gestionar > Vista de sistema > Panel de control de salud de despliegue.

La tabla siguiente resume los tipos de datos disponibles para cada una de las vistas de salud de despliegue.

Tabla 1. Resumen de vistas de salud de despliegue

	Panel de control	**Topología**	**Tabla**
Utilización de unidad	✔	✔	✔
Alertas de correlación	✔		
Autosupervisión	✔		
Requisitos del sistema	✔		
Agregación		✔	✔
Motores de inspección (datos de verificación de S-TAP)		✔	
Conectividad		✔	✔
Conectividad de S-TAP		✔	

Atención: Las vistas de salud de despliegue presentan los datos recopilados de todo un entorno de Guardium y están disponibles sólo desde un gestor central.

- Configuración de un gestor central para las vistas de salud de despliegue
  Para utilizar las vistas de salud de despliegue, habilite la recopilación de datos de utilización de unidad, configure alertas de correlación y configure la importación y exportación de datos para el entorno.
- Vistas de tabla y topología de salud de despliegue
  Obtenga más información sobre cómo las vistas de tabla y topología de salud de despliegue presentan la configuración del entorno de Guardium y sus datos.
- Panel de control de salud de despliegue
  Obtenga más información sobre cómo el panel de control de salud de despliegue presenta los datos de todo el despliegue de Guardium.
- Escenario: Resolución de problemas de sistemas sobrecargados mediante la vista de topología de salud de despliegue
  En este tema se describe la utilización de la vista de topología de salud de despliegue para identificar y arreglar un sistema sobrecargado del entorno.

Tema principal: Utilización de las funciones de Gestión central

Configuración de un gestor central para las vistas de salud de despliegue

Para utilizar las vistas de salud de despliegue, habilite la recopilación de datos de utilización de unidad, configure alertas de correlación y configure la importación y exportación de datos para el entorno.

Acerca de esta tarea

Desde un gestor central, las vistas de salud de despliegue muestran datos de todo un entorno de Guardium. La capacidad de visualizar datos sobre todo un despliegue requiere la recopilación de datos de utilización de unidad, la configuración de alertas de correlación y que la importación, exportación y verificación de S-TAP de datos estén correctamente configuradas. Para ver un resumen de los datos que se muestran en las vistas de salud de despliegue, consulte Vistas de salud de despliegue.

Es probable que el despliegue ya está configurado para dar soporte a las vistas de salud de despliegue. Compruebe los pasos de configuración que se describen en este procedimiento si se encuentra alguno de los problemas siguientes en alguna de las vistas de salud de despliegue:

- Informe de uso del almacenamiento intermedio de CM no planificado
- Informe de utilización de la unidad no planificado
- Exportación no planificada
- Importación no planificada
- No se han encontrado problemas
- Estado no disponible

Procedimiento

1. Configure la recopilación y el proceso de los datos de utilización de unidad desde el gestor central. Para obtener más información, consulte Configuración del proceso de datos de utilización de unidad.
2. Habilite alertas de correlación para la inclusión en el panel de control de salud de despliegue.
   a. Abra Proteger > Protección de intrusión de base de datos > Creador de alertas.
   b. Seleccione una alerta existente y pulse el icono , o cree una nueva alerta pulsando el icono .
   c. Proporcione una Categoría para la alerta. Las alertas sin una categoría especificada se muestran como Sin categorizar.
   d. Marque el recuadro de selección Ver en un panel de control de salud de despliegue para incluir la alerta en el panel de control.
   Atención: Las alertas deben tener la Gravedad establecida en BAJA, MEDIA o ALTA para que se incluyan en el panel de control de salud de despliegue.
   Para obtener más información sobre la definición de alertas, consulte Creación de alertas.
3. Configure la importación y exportación de datos desde el gestor central. Para obtener más información, consulte Agregación.
   Consejo: Utilice la herramienta Distribuir perfiles de configuración para simplificar el proceso de configuración de la importación y exportación de datos para un despliegue de Guardium. Para obtener más información, consulte Utilización de perfiles de configuración.
4. Configure la verificación de S-TAP para todos los S-TAP soportados. Para obtener más información, consulte Supervisor de estado de S-TAP y Visualización de los resultados de verificación de S-TAP.

Resultados

Cuando haya completado los procedimientos de configuración y permitido la actualización de los datos, las vistas Topología de salud de despliegue y Tabla de salud de despliegue mostrarán principalmente el estado excepto para los sistemas con problemas de salud ya existentes. El panel de control de salud de despliegue incluirá los problemas de utilidad de unidad ya existentes y empezará mostrando las nuevas condiciones de alerta de correlación.

Cuando altere la utilización de unidad o las planificaciones de importación o exportación de datos, espere una hora para permitir que las vistas de salud de despliegue se actualicen con la nueva información. La disponibilidad de los nuevos datos de alerta de correlación depende de la frecuencia de notificación especificada para una alerta.

Tema principal: Vistas de salud de despliegue
Conceptos relacionados:
Agregación
Tareas relacionadas:
Configuración del proceso de datos de utilización de unidad
Utilización de perfiles de configuración
Información relacionada:
Alertas de correlación

Vistas de tabla y topología de salud de despliegue

Obtenga más información sobre cómo las vistas de tabla y topología de salud de despliegue presentan la configuración del entorno de Guardium y sus datos.

Se puede acceder desde cualquier gestor central a la vista de topología de salud de despliegue, donde se proporciona una visualización rápida de todo el entorno de Guardium conectado a ese gestor central. Además de mostrar las relaciones entre nodos del entorno, la vista de topología de salud de despliegue también proporciona información de salud sobre todos los agregadores, recopiladores y S-TAPs conectados. Hay varias acciones de investigación y resolución disponibles directamente desde la vista de topología de salud de despliegue de destino para ayudarle a resolver rápidamente los problemas de salud descubiertos en el entorno.

La vista de topología de salud de despliegue predeterminada es una vista de flujo de datos que muestra las relaciones de importación y exportación de datos entre agregadores y unidades gestionadas. Abra la vista de topología de salud de despliegue en Gestionar > Vista de sistema > Topología de salud de despliegue.

También hay disponible una vista de tabla clasificable de los datos de salud de despliegue en Gestionar > Vista de sistema > Tabla de salud de despliegue.

Disponibilidad de datos

Varios factores influyen en la disponibilidad de los datos del sistema y en cómo estos datos se visualizan en las vistas de tabla y topología de salud de despliegue. Para obtener información sobre cómo configurar el sistema para utilizar las vistas de salud de despliegue, consulte Configuración de un gestor central para las vistas de salud de despliegue.

Tipos de datos

Cuando se han configurado correctamente, las vistas de tabla y topología de salud de despliegue muestran datos recopilados de distintos orígenes. Los tipos específicos de datos que se visualizan dependen del tipo de unidad, tal como se resume en las secciones siguientes.

Conectividad

La categoría de conectividad indica si los sistemas de un entorno de Guardium pueden comunicarse.

- Se aplica a gestores centrales, agregadores, recopiladores y S-TAPs
- Por ejemplo, una unidad que no responde y un S-TAP que no responde

Utilización de unidad

La categoría de utilización de unidad proporciona información sobre el nivel de carga de los sistemas Guardium.

- Se aplica a gestores centrales, agregadores y recopiladores
- Por ejemplo, carga de CPU, espacio de almacenamiento intermedio libre y uso de disco de MySQL
- Para obtener más información, consulte Nivel de utilización de unidad.

Agregación

La categoría de agregación proporciona información sobre el flujo de importación y exportación de datos entre sistemas Guardium.

- Se aplica a gestores centrales (si están configurados como agregadores), agregadores y recopiladores
- Por ejemplo, la importación ha fallado, la exportación ha fallado y exportación no planificada
- Para obtener más información, consulte Informes de administración predefinidos y Agregación.

Motores de inspección

La categoría Motores de inscripción proporciona información de verificación de S-TAP.

- Se aplica a S-TAPs
- Por ejemplo, la verificación de S-TAP ha fallado
- Para obtener más información, consulte Configuración de la planificación de verificación de S-TAP y Visualización de los resultados de verificación de S-TAP.

Pulse el icono para abrir el recuadro de diálogo Personalizar valores para definir los tipos de datos que se muestran en las vistas de tabla y topología de salud de despliegue.

Latencia de datos

Varias planificaciones definidas por el usuario y preestablecidas determinan la latencia de datos que se visualiza en la vista de topología de salud de despliegue. Estas planificaciones se resumen en la tabla siguiente.

Tabla 1. Latencia de datos de vista de topología de salud de despliegue

Categoría de salud	Tipo de nodo	Latencia
Conectividad	Agregador o recopilador	Menos de 15 minutos
Conectividad	S-TAP	Menos de 15 minutos si el equilibrio de carga empresarial está habilitado Menos de 1 hora si el equilibrio de carga empresarial no está habilitado
Agregación	Gestor central, agregador o recopilador	Menos de 1 hora
Verificación	S-TAP	Menos de 1 hora
Utilización de unidad	Gestor central, agregador o recopilador	1 - 2 horas, según la configuración recomendada. Para obtener más información, consulte Configuración del proceso de datos de utilización de unidad.

Observe las latencias siguientes para cambios específicos de la configuración o del entorno:

- Los agregadores o recopiladores que se acaban de registrar pasan a estar disponibles para las vistas de salud de despliegue al cabo de 15 minutos.
- La supresión de la planificación de exportación de datos o la configuración de exportación de datos de un recopilador se refleja en las vistas de estado de despliegue al cabo de 2 horas.

Presentación de datos

Estado de salud

La vista de topología de salud de despliegue muestra tres categorías de información de salud para los sistemas Guardium: conectividad, utilización de unidad y agregación. A las métricas de estas categorías se les asigna uno de los estados de salud siguientes: estado no disponible (menos grave), sin problemas de salud, gravedad baja, gravedad media y gravedad alta (más grave). El estado general se determina según el estado más grave de cualquier métrica individual incluida en cualquiera de las categorías de salud que se muestran. Los datos que se han excluido utilizando el recuadro de diálogo Personalizar valores no se utilizan para determinar el estado general de un sistema.

Por ejemplo, si se asigna a la métrica Reinicios en la categoría Utilización de unidad un estado de Gravedad alta, pero no existen problemas de salud en otra categoría, el Estado general de ese sistema será Gravedad alta. Este comportamiento garantiza que la condición más grave siempre se visualice rápidamente como el estado general de un sistema.

En la vista Gestionar > Vista de sistema > Topología de salud de despliegue, sólo se muestran los estados detallados para las categorías de salud disponibles cuando se encuentra al menos un problema de gravedad baja, media o alta.

En la vista Gestionar > Vista de sistema > Tabla de salud de despliegue, siempre se muestran los estados detallados para las categorías de salud disponibles.

Resumen de estado de salud

La vista de topología de salud de despliegue implementa una estrategia de resumen de estado de salud para mostrar eficazmente la información de salud de todo un entorno de Guardium. Con esta estrategia, los nodos hijo se contraen bajo sus nodos padre, y el estado de salud del hijo se resume en el padre. El estado resumido se expresa como un icono pequeño adjunto al nodo padre.

Atención: El resumen de estado de salud sólo está soportado para nodos de S-TAP que resuman el estado en su recopilador padre.

Por ejemplo, indica un recopilador sin problemas de salud, pero el pequeño círculo rojo indica que uno o más S-TAPs asociados con ese recopilador tienen problemas de gravedad alta. Al pulsar el recopilador, el nodo se expande y revela los S-TAPs asociados y su estado de salud. Por ejemplo,

rojos y dos amarillos indica cuatro S-TAPs asociados con el recopilador: dos S-TAPs tienen problemas de salud de gravedad alta y dos S-TAPs tienen problemas de salud de gravedad baja.

Cuando se contraen los nodos hijo, sólo el estado más grave se resume del nodo hijo al nodo padre. En el ejemplo anterior, el nodo padre muestra un círculo rojo porque uno o varios de sus hijos tienen problemas de gravedad alta. Sin embargo, si uno o varios nodos hijo contienen problemas de gravedad baja, pero ninguno de los otros nodos hijo tienen problemas de salud, el nodo padre mostraría un pequeño círculo amarillo.

Presentación del despliegue

Algunas configuraciones de despliegue se muestran inesperadamente en la vista de topología de salud de despliegue. Varios de estos escenarios de configuración se describen en las secciones siguientes.

Unidades gestionadas anteriores a Guardium V10.1.3

Es posible que las unidades gestionadas anteriores a Guardium V10.1.3 muestren datos de utilización de unidad incorrectos o incoherentes cuando se conecten a un gestor central de la versión V10.1.3 o posterior. Para corregir el problema, inicie sesión en la CLI del gestor central y ejecute el mandato siguiente para cada unidad gestionada:

```
grdapi change_tracker_reset host=[nombre de host o dirección IP de unidad gestionada]
```

Práctica recomendada: En un entorno gestionado, se recomienda que todas las unidades operen en el mismo nivel de versión de Guardium.

Unidades gestionadas anteriores a Guardium V10.1

Las unidades gestionadas anteriores a Guardium V10.1 muestran Estado no disponible en la sección de salud de Agregación cuando se visualiza desde la página Topología de salud de despliegue o la Tabla de salud de despliegue.

Práctica recomendada: En un entorno gestionado, se recomienda que todas las unidades operen en el mismo nivel de versión de Guardium.

S-TAP no soportados

La vista de topología de salud de despliegue muestra los S-TAP configurados para verificación de S-TAP o que participan en el equilibrio de carga empresarial. Si no se puede configurar un S-TAP para la verificación de S-TAP o para participar en el equilibrio de carga empresarial, los S-TAP no se mostrarán.

Equilibrio de carga de S-TAP

Si el equilibrio de carga de S-TAP está configurado con el parámetro participate_in_load_balancing y un S-TAP está configurado para equilibrar el tráfico entre varios recopiladores, la vista de topología de salud de despliegue muestra ese S-TAP como un nodo hijo de ese recopilador. Por ejemplo, si *S-TAP 1* tiene equilibrio de carga con *Recopilador A* y *Recopilador B*, tanto *Recopilador A* como *Recopilador B* muestran *S-TAP 1* como hijo en la vista de topología de salud de despliegue.

Unidades no gestionadas

Si un recopilador exporta datos a un gestor central o a un agregador que está configurado como un gestor central, pero este recopilador no está designado como una unidad gestionada de ese clúster de gestión central, el Estado global del recopilador en la vista de topología de salud de despliegue se muestra como Estado de salud no disponible. Cuando se despliega la vista de topología de salud de despliegue, ninguna información adicional sobre el recopilador pasa a estar disponible, a menos que el recopilador esté designado como una unidad gestionada del gestor central.

Recopilador que exporta datos a hosts primarios y secundarios

Cuando un recopilador está configurado para exportar datos a hosts primarios y secundarios, sólo se utiliza el host primario para la vista de topología de salud de despliegue.

Tema principal: Vistas de salud de despliegue
Tareas relacionadas:
Configuración de un gestor central para las vistas de salud de despliegue

Panel de control de salud de despliegue

Obtenga más información sobre cómo el panel de control de salud de despliegue presenta los datos de todo el despliegue de Guardium.

Disponibilidad de datos

Varios factores afectan a la disponibilidad y latencia de los datos de salud y cómo estos datos se muestran en el panel de salud de despliegue. La tabla siguiente resume los datos incluidos en el panel de control, los criterios de desencadenante y la información de depuración y latencia de datos.

Tabla 1. Resumen de los datos del panel de control de salud de despliegue

Origen de datos	Tipo de información	Criterios de desencadenante	Latencia de datos	Intervalo de depuración de datos
Recursos del sistema	Configuración del sistema, por ejemplo, núcleos de CPU, memoria del sistema, capacidad de disco /var	El sistema no cumple los requisitos mínimos	Se actualiza siempre que se inicia o reinicia el servidor de la interfaz de usuario	No aplicable
Utilización de unidad	Datos de utilización de unidad como, por ejemplo, reinicios del sniffer, uso de disco de MySQL y carga de CPU.	El valor supera los umbrales de utilización de unidad	Se actualiza en 1 o 2 horas, según la configuración recomendada. Para obtener más información, consulte Configuración del proceso de datos de utilización de unidad.	Los datos de utilización de unidad se depuran después de 60 días Los datos de uso almacenamiento intermedio de sniffer se depuran después de 14 días
Autosupervisión del sistema	Uso de disco de MySQL y uso de disco del sistema	El uso cumple o supera los umbrales predeterminados (75 % para gravedad alta, 90 % para gravedad crítica)	Se actualiza cada 5 - 10 minutos. Para la gravedad alta, si el mismo suceso se produce varias veces en un periodo de 15 minutos, la indicación de fecha y hora se actualiza para reflejar la última instancia. Si el mismo suceso se produce después de un intervalo de 15 minutos, se crea una entrada nueva con la última indicación de fecha y hora. Para los problemas críticos, cada una de las instancias de un suceso se crea con una indicación de fecha y hora exclusiva.	Los problemas de alta gravedad se depuran después de 7 días Los problemas críticos no se depuran nunca
Alertas de correlación	Alertas de correlación desencadenadas	Se ha alcanzado un umbral de alerta	Se actualiza según la frecuencia de notificación de alerta. Para obtener más información, consulte Alertas de correlación.	Los datos se depuran después de 7 días

Importante:

- Sólo se incluyen en el panel de control de salud del despliegue los datos de los sistemas que ejecutan Guardium V10.1.2 y posteriores.
- Cuando cambia el nombre de host de un sistema, los datos ya existentes asociados con el nombre de host original dejan de visualizarse en el panel de control de salud de despliegue.
- Cuando un gestor central primario transfiere datos a un gestor central secundario durante un escenario de sustitución por anomalía, hasta 30 minutos de datos no están disponibles para el panel de control de salud de despliegue.

Presentación de datos

El panel de control de salud de despliegue formatea y presenta los datos mediante diversos contenedores, similares a pequeñas ventanas o áreas. La tabla siguiente resume los datos que se presentan en cada área del panel de control.

Tabla 2. Resumen de las áreas del panel de control de salud de despliegue

	Nombre del área						
Origen de datos	**Requisitos de recursos**	**Problemas de utilización de unidad**	**Gráficos de tiempo de utilización de unidad**	**Alertas (por categoría, nombre, gravedad o sistema)**	**Sucesos**	**Gravedad alta**	**Crítico**
Recursos del sistema	✔					✔	
Utilización de unidad		✔	✔		✔	✔	
Autosupervisión del sistema					✔	✔ (Cuando el uso cumple o supera el umbral del 75 %)	✔ (Cuando el uso cumple o supera el umbral del 90 %)
Alertas de correlación				✔	✔	✔	
Las áreas siguientes se muestran de forma predeterminada: *Alertas por nombre*, *Problemas críticos*, *Línea temporal de sucesos*, *Problemas de gravedad alta* y *Problemas de utilización de unidad*.							

Filtro del panel de control

El filtro del panel de control permite un filtrado rápido de los datos según los sistemas Guardium, la gravedad de los problemas y el periodo de tiempo. Los valores de filtro afectan a los datos que aparecen en todo el panel de control a menos que se indique lo contrario.

El filtro de los sistemas Guardium permite el filtrado del panel de control por tipo de unidad o por grupos definidos en Gestionar > Gestión central > Grupos de unidades gestionados.

De forma predeterminada, el panel de control muestra todos los problemas disponibles: baja, media, alta y crítica. Utilice el menú Gravedad para filtrar los datos en el panel de control por gravedad. Si se selecciona alta se filtrará todo el panel de control para que muestre sólo los problemas de gravedad alta. Si se selecciona crítica se filtrará todo el panel de control para que muestre sólo los problemas críticos. Es posible seleccionar problemas con gravedad alta y crítica para filtrar todos los datos de menor gravedad.
Notas:

- Los problemas críticos pendientes o no resueltos se muestran en el panel de control independientemente del valor de filtro Gravedad.
- Para el área *Problemas de utilización de unidad*, el filtro Gravedad del panel de control se basa en la gravedad de utilización de unidad global. Para obtener más información sobre cómo se asigna la gravedad de utilización de unidad, consulte Problemas de utilización de unidad.

El filtro de tiempo determina el rango de datos que se visualizará en el panel de control. Los valores predeterminados permiten periodos de tiempo de 1 hora a 3 semanas, pero también se da soporte a periodos de tiempo personalizados. El filtro de tiempo no se aplica a problemas críticos: los problemas críticos se visualizan siempre, independientemente del valor de filtro de tiempo.

Utilice el menú Añadir gráfico para añadir áreas al panel de control o sustituir áreas predeterminados que haya eliminado anteriormente.

Resumen del panel de control

El resumen del panel de control proporciona recuentos globales de los problemas de salud que se han detectado en el despliegue de Guardium. Los recuentos de Recopiladores con problemas y Agregadores con problemas indican el número de sistemas (recopiladores y agregadores) que se han detectado con problemas de salud. Los recuentos de Crítica y Alta indican el número de problemas detectados en todos los sistemas incluidos en el panel de control.
Nota:

- Si se añaden o eliminan áreas del panel de control, esto no afecta a los recuentos de Crítica y Alta.
- Los recuentos de la barra de resumen del panel de control reflejan los valores de filtro del panel de control.

Alertas por categoría, nombre, gravedad o sistema

El panel de control de salud de despliegue da soporte a varias áreas según las alertas de correlación de Guardium: *Alertas por categoría*, *Alertas por nombre*, *Alertas por gravedad* y *Alertas por sistema*. Añada áreas de alerta de correlación al panel de control mediante el menú Añadir gráfico.

Las alertas de correlación se deben configurar explícitamente para su inclusión en el panel de control de salud de despliegue. Para obtener información sobre cómo configurar alertas para el panel de control, consulte Configuración de un gestor central para las vistas de salud de despliegue.

Requisitos de recursos

El área *Requisitos de recursos* indica si los sistemas en un despliegue de Guardium cumplen los requisitos mínimos de hardware para CPU, memoria y capacidad de disco /var. Cualquier recurso del sistema que no cumpla el requisito mínimo se designa como un problema de gravedad alta y aparece en el área *Requisitos de recursos* y el área *Problemas de gravedad alta*.

Utilice el recuadro de selección Incluir sistemas en buen estado en la vista de detalles del área para incluir todos los datos disponibles para los sistemas y el marco de tiempo indicados en la barra de filtro del panel de control. Incluyendo todos los datos disponibles, el recuadro de selección Incluir sistemas en buen estado prevalece sobre el valor Gravedad del filtro global del panel de control. De forma predeterminada, los sistemas sin problemas de salud detectados se excluyen.

También hay disponible una tabla que visualiza todos los requisitos de recursos que se cumplen y que no se cumplen en el despliegue de Guardium en Gestionar > Gestión central > Recursos del sistema.
Nota:

- Los problemas de recursos del sistema no se visualizan en la línea temporal *Sucesos* porque no están asociados con una indicación de fecha y hora específica.

Problemas de utilización de unidad

El área *Problemas de utilización de unidad* muestra los problemas según los umbrales de utilización de unidad. Los problemas que se visualizan en el área representan métricas individuales que superan sus respectivos umbrales. La gravedad global se asigna según el problema de gravedad más alta que se encuentra en todas las métricas disponibles para un sistema individual en un periodo de tiempo especificado. Para obtener más información sobre los umbrales de utilización de unidad, consulte Nivel de utilización de unidad.

La vista de detalles del área *Problemas de utilización de unidad* incluye una hora de Inicio de periodo y una Indicación de fecha y hora:

- La hora de Inicio de periodo indica que los datos *Supervisor de uso de almacenamiento intermedio de CM* se resumen en periodos de una hora, por ejemplo, periodos a partir de las 13:00, 12:00 y 11:00.
- La Indicación de fecha y hora indica cuándo los datos de niveles de utilización de unidad se añaden al panel de control de salud de despliegue, según la planificación de niveles de utilización de unidad o mediante *Ejecutar una vez ahora*.

Para obtener más información, consulte Configuración del proceso de datos de utilización de unidad.
La primera vez que los datos de utilización de unidad se llevan al panel de control de salud de despliegue, todos los datos de utilización de unidad tienen la misma *indicación de fecha y hora* pero distintas horas de *Inicio de periodo*. Con el tiempo, las indicaciones de fecha y hora aparecerán en intervalos según la planificación de niveles de utilización de unidad. Por ejemplo, si los datos de niveles de utilización de unidad se recopilan cada 40 minutos después de la hora, verá los valores de *hora de inicio de periodo* e *indicación de fecha y hora* de la forma siguiente:

Tabla 3. Valores de ejemplo de hora de inicio de periodo y de indicación de fecha y hora de utilización de unidad

Inicio de periodo	Indicación de fecha y hora
13:00	14:40
12:00	13:40
11:00	12:40

Utilice el recuadro de selección Incluir sistemas en buen estado en la vista de detalles del área para incluir todos los datos disponibles para los sistemas y el marco de tiempo indicados en la barra de filtro del panel de control. Incluyendo todos los datos disponibles, el recuadro de selección Incluir sistemas en buen estado prevalece sobre el valor Gravedad del filtro global del panel de control. De forma predeterminada, los sistemas sin problemas de salud detectados se excluyen.

Gráficos de tiempo de utilización de unidad

Los *gráficos de tiempo de utilización de unidad* permiten la observación de tendencias en datos de utilización de unidad a lo largo del tiempo. Los *gráficos de tiempo de utilización de unidad* se pueden configurar para mostrar varias métricas de utilización de unidad para un único sistema Guardium o para mostrar una única métrica de utilización de unidad para varios sistemas Guardium.

Los *gráficos de tiempo de utilización de unidad* se estructuran según los criterios siguientes:

- El eje x representa la hora de *inicio de periodo*
- Cuando se representan varias métricas en un gráfico y los valores de las métricas están en el mismo rango, se traza un eje y. Por ejemplo, *Uso de disco de MySQL* y *Uso de disco de /var* se expresan como porcentajes y se dibujan con el mismo eje y.
- Cuando se representan varias métricas en un gráfico y los valores de las métricas no son similares, se trazan dos ejes y. Por ejemplo, *Uso de disco de MySQL* se expresa como un porcentaje y *Solicitudes de proceso flat log* se expresa como un entero, así que se dibujan dos ejes y: uno que muestra los porcentajes y otro que muestra los enteros.
- Si el valor de una métrica queda fuera del rango de un eje y, ese valor se visualiza en la parte inferior del gráfico. Este comportamiento acomoda escenarios donde se expresan dos métricas distintas con unidades similares pero valores considerablemente distintos: por ejemplo, enteros en el rango de miles versus millones. Consejo: Cree varios gráficos de tiempo cuando los valores estén en rangos considerablemente distintos.

Nota: Los sistemas no se incluyen en el menú Valores de gráfico de tiempo > Nombre de host cuando los datos de utilización de unidad no existen para el sistema en el marco de tiempo especificado en la barra de filtro del panel de control.
Tema principal: Vistas de salud de despliegue
Tareas relacionadas:
Configuración de un gestor central para las vistas de salud de despliegue
Configuración del proceso de datos de utilización de unidad

Escenario: Resolución de problemas de sistemas sobrecargados mediante la vista de topología de salud de despliegue

En este tema se describe la utilización de la vista de topología de salud de despliegue para identificar y arreglar un sistema sobrecargado del entorno.

Acerca de esta tarea

Este escenario implica identificar los problemas de salud desde la vista de topología de salud de despliegue, asesorar sobre la causa raíz y correlacionar esa evaluación con datos adicionales antes de resolver el problema y verificar el arreglo. El ejemplo que se describe aquí implica un recopilador sobrecargado, pero el proceso es aplicable para otros casos.

Procedimiento

1. En un gestor central, vaya a Gestionar > Vista de sistema > Topología de estado de despliegue.
2. Revise la topología de despliegue y evalúe la salud global de los sistemas del entorno. En un nivel alto, los iconos indican sistemas sanos, mientras que los iconos y indican sistemas con algunos problemas de salud.
3. Si ve sistemas con iconos de estado o , pulse el nodo para ver una superposición con información de salud adicional.
4. Utilice la información que se presenta en la superposición del nodo para empezar a diagnosticar los problemas de salud. Por ejemplo, un recopilador con estados de gravedad media o alta para Uso de disco de /var, Reinicios, Cola de analizador y Cola de registrador indica que el recopilador está sobrecargado.
5. Tras evaluar inicialmente los problemas de salud desde la vista de topología de salud de despliegue, intente correlacionar los resultados con datos adicionales. Por ejemplo, si sospecha que un sistema está sobrecargado, empiece supervisando el tráfico de ese sistema.
6. Cuando tenga la certeza de que ha diagnosticado los problemas de salud subyacentes, realice las acciones correctivas. En el ejemplo de un sistema sobrecargado, podría establecer equilibrio de carga empresarial o reasignar S-TAPs a otro recopilador. Normalmente este conjunto de síntomas no se producirá si el equilibrio de carga empresarial ya se ha configurado y está en uso.
7. Tras realizar las acciones correctivas, el estado del nodo en la vista de topología de salud de despliegue se actualizará tras la siguiente renovación de los datos de supervisor de uso de almacenamiento intermedio de gestor central y de utilización de unidad. Este intervalo de renovación depende de la planificación de los datos de utilización de unidad de proceso.

Tema principal: Vistas de salud de despliegue

Inventario de despliegue

La vista de inventario proporciona una vista centralizada de todos los servidores de base de datos y de los clientes GIM o S-TAP instalados.

Tema principal: Utilización de las funciones de Gestión central

Vista Despliegue de recursos

La vista Despliegue de recursos proporciona una vista centralizada de todos los servidores de base de datos y sus recopiladores, agregadores y gestores centrales asociados.

Tema principal: Utilización de las funciones de Gestión central

Creación de grupos de unidades gestionadas

Organice las unidades gestionadas en grupos y, a continuación, realice acciones en estos grupos.

Acerca de esta tarea

Los grupos de unidades gestionadas le permiten organizar las unidades gestionadas en grupos significativos y, a continuación, realizar acciones en esos grupos. Por ejemplo, puede crear grupos de unidades gestionadas para tipos de unidades, geografías o líneas de negocio específicos. Las acciones que puede llevar a cabo incluyen la instalación de políticas, la distribución de parches o la configuración en un grupo de unidades gestionadas.

Procedimiento

1. Vaya a Gestionar > Gestión central > Grupos de unidades gestionadas.
2. En la página Grupos de unidades gestionadas, pulse para crear un nuevo grupo de unidades gestionadas o para editar un grupo existente.
3. En el recuadro de diálogo Crear nuevo grupo de unidades gestionadas, especifique un nombre para el grupo en el campo Nombre de grupo.
   Recomendación: Para garantizar la compatibilidad con otros componentes de Guardium, no utilice espacios ni caracteres especiales en los nombres de grupo.
4. Utilice los iconos para seleccionar unidades gestionadas para incluirlas en el grupo.
5. Cuando haya terminado de seleccionar las unidades gestionadas que desea incluir en el grupo, pulse el botón Guardar. El nuevo grupo de unidades gestionadas se guardará y aparecerá en la página Grupos de unidades gestionadas.
6. Opcionalmente, en la página Grupos de unidades gestionadas, pulse el icono para expandir el grupo y ver sus unidades gestionadas.

Resultados

Una vez que se ha definido un grupo de unidades gestionadas, este está disponible en la página Gestionar > Gestión central > Gestión central, la página Gestionar > Gestión central > Distribuir perfiles de configuración, como un grupo de unidades gestionadas en la herramienta Gestionar > Gestión central > Equilibrio de carga empresarial > Asociar S-TAP y unidades gestionadas y en otras ubicaciones donde se utilizan los grupos de unidades gestionadas.

Tema principal: Utilización de las funciones de Gestión central

Supervisión de unidades gestionadas

Supervise las unidades gestionadas mediante la gestión central.

Para supervisar unidades gestionadas:

1. Inicie sesión como usuario de administración en la interfaz gráfica de usuario de Guardium de la unidad que se gestionará.
2. Pulse Informes > Informes operativos de Guardium > Unidades gestionadas para abrir Unidades gestionadas.

En la tabla siguiente se describe cada uno de los componentes del panel Gestión central.

Tabla 1. Supervisión de unidades gestionadas

Control	Descripción
Recuadro de selección Seleccionar todo	Marque este recuadro del área sombreada de la primera columna para seleccionar todas las unidades compartidas.
Deseleccionar todo	Desmarque todas las unidades gestionadas.
Recuadro de selección	Marque este recuadro para seleccionar la unidad para la operación que desee.
Renovar información de unidad	Renueva toda la información que se muestra en la vista expandida de esa unidad y emite nuevas solicitudes a esa unidad. Esta acción también causa un ciclo de sincronización de usuario completo.
Rearrancar unidad	Rearranca la unidad a nivel del sistema operativo. De forma predeterminada, el portal de Guardium se inicia durante el arranque.
Reiniciar portal de unidad	Reinicia el portal de aplicación de Guardium en la unidad gestionada. A continuación, puede iniciar sesión en esa unidad para realizar tareas de Guardium (por ejemplo, definir o eliminar motores de inspección).
Ver atributos SNMP de unidad	Abra el panel Visor de SNMP en una ventana aparte. Al pulsar el icono Renovar en el panel Visor de SNMP los datos de la ventana se renuevan.
Ver syslog	Abre el visor syslog en una ventana aparte, que muestra los últimos 64 KB de mensajes de syslog. Al pulsar el icono Renovar en el panel Visor de syslog los datos de la ventana se renuevan.
Atajo a portal de unidad	Abre la página de inicio de sesión de Guardium para la unidad gestionada en una ventana de navegador aparte.
Nombre de unidad	Nombre de host de la unidad gestionada. Si mantiene pulsado el puntero del ratón sobre el nombre de unidad, su dirección IP se muestra como una ayuda contextual. Si el nombre de host cambia en la unidad, el Gestor central ya no verá esa unidad cuando renueve automáticamente el estado En línea. Si sospecha que el nombre de host ha cambiado, utilice Renovar en la barra de herramientas. Obtenga el nombre de host cambiado y actualice el estado En línea actual y otra información de esa unidad que se muestre.
En línea	Indica si la unidad está en línea. Si el indicador verde está encendido, la unidad está en línea; si el indicador rojo está encendido, la unidad está fuera de línea. El Gestor central renueva este estado con el intervalo de renovación especificado en la configuración de gestión central (de forma predeterminada, 1 minuto). Si se ha producido un error al conectarse a una unidad, la descripción del error se puede visualizar como una ayuda contextual. Pase el puntero del ratón por encima del registro de esa unidad en la tabla de gestión.

Control	Descripción
Motores de inspección	Pulse el icono ⊞ para expandir la lista de motores de inspección; pulse el icono ⊟ para ocultar la lista de motores de inspección. A partir de aquí, según el estado, podrá detener o iniciar el motor de inspección. La información que se muestra para cada motor de inspección es la siguiente (esta información se obtiene de la unidad gestionada cuando se pulsa Renovar, no en cada ejecución de ping): Nombre: nombre del motor de inspección. Protocolo: protocolo que supervisa el motor de inspección: Oracle, MSSQL, Sybase, Informix o DB2 Activo al iniciar: indica si el motor de inspección se inicia cuando arranca el sistema. Ejecutar desde IP: Indica si la lista de direcciones Desde-IP se va a excluir (no examinar). Desde-IP/Máscara: Lista de las direcciones IP y máscaras de subred de los clientes cuyo tráfico de base de datos a las direcciones A-IP/Máscara supervisa el motor de inspección. Puertos: Puertos en los que se comunican los clientes y servidores de base de datos; puede ser un solo puerto, una lista de puertos o un rango de puertos. A-IP/Máscara: Lista de direcciones IP y máscaras de subred de servidores cuyo tráfico desde la máquina cliente correspondiente (Desde-IP/Máscara) se supervisa.
Política de seguridad instalada	Nombre de la política de seguridad instalada en la unidad gestionada. Este campo se actualiza en cada ping.
Modelo	Número de modelo de Guardium de la unidad gestionada.
Versión	Número de versión de Guardium de la unidad gestionada.
Último parche	Último parche instalado.
Tiempo del último ping	Última vez que se el Gestor central ejecutó ping a la unidad para determinar el estado en línea/fuera de línea de la unidad gestionada.
Unidades seleccionadas	
Configuración de grupo	Configuración de grupo abre una nueva ventana que permite que el usuario mantenga grupos, cree nuevos grupos, elimine grupos y asocie unidades gestionadas con grupos.
Desregistrar	Desregistra todas las unidades seleccionadas.
Reiniciando	
Rearrancar	Rearranca las unidades seleccionadas.
Reiniciar Portal	Reinicia el portal seleccionado.
Reiniciar motores de inspección	Reinicia los motores de inspección de las unidades seleccionadas.
Distribución	
Renovar	Renueva las unidades seleccionadas.
Instalar política	El nombre de política es un enlace que abre una nueva ventana con el detalle de la política.
Distribuir parches	Distribución de parches abre una nueva pantalla, muestra una lista de parches disponibles con dependencias y permite seleccionar un parche e instalarlo en todas las unidades. Planifique la aplicación de parche hasta con un año de antelación.
Distribuir archivos Jar subidos	Pulse Reforzar > Asesoramiento de vulnerabilidades > Subidas de cliente. A continuación, especifique el nombre del archivo que se va a subir. De lo contrario, pulse Examinar para localizar y seleccionar ese archivo. Suba un controlador cada vez. Pulse Subir. Cuando la operación se complete se le notificará y el archivo subido se mostrará. Esta acción lleva el archivo subido al Gestor central. Marque los recuadros de selección de la unidad o unidades gestionadas donde se van a distribuir estos archivos JAR. Pulse Distribuir archivos Jar subidos.
Distribuir valores de copia de seguridad de parches	Este ajuste distribuye lo siguiente a las unidades seleccionadas: PATCH_BACKUP_FLAG; PATCH_AUTOMATIC_RECOVERY_FLAG; PATCH_BACKUP_DEST_HOST; PATCH_BACKUP_DEST_DIR; PATCH_BACKUP_DEST_USER; PATCH_BACKUP_DEST_PASS
Distribuir configuración de autenticación	Seleccione las unidades gestionadas que recibirán la distribución de la autenticación de Gestión central. Pulse Distribuir configuración de autenticación para distribuir la configuración de autenticación a todas las unidades gestionadas seleccionadas.

Control	Descripción
Distribuir configuraciones	Se distribuyen las configuraciones siguientes para sincronizar los parámetros entre el Gestor central y las unidades gestionadas: • Detección de anomalías: Activo al iniciar, Intervalo de sondeo • Alertador: todos los campos • Archivado de datos: todos los campos • Perfil global: inicios de sesión simultáneos, seguridad a nivel de datos, todos los campos, excepto Plantillas con nombre (que ya están sincronizadas), texto de pie de página de TPDF e imagen de logotipo • Creación de alias IP-Nombre de host: Ambos recuadros de selección • Archivado de resultados: Todos los campos • Exportación de resultados: Todos los campos • Inferencia de sesiones: Todos los campos • Copia de seguridad del sistema: Todos los campos • Exportación de datos: Todos los campos Algunas de estas configuraciones no entran en vigor hasta que se reinicia el portal (Detección de anomalías, Inferencia de sesión). Otros procesos, por ejemplo, el alertador, se debe reiniciar, ya sea directamente mediante el portal admin de la unidad gestionada, o rearrancando todas las unidades gestionadas relevantes desde el gestor. Distribuir configuraciones no reinicia las unidades gestionadas. Hay un icono individual para reiniciar cada unidad gestionada. Reiniciar Portal reinicia todas las unidades seleccionadas. Después de la distribución, se visualizará un mensaje que indica que las unidades gestionadas deberán reiniciarse para que todas las configuraciones entren en vigor en las unidades gestionadas. Cada parámetro con planificación tiene un segundo recuadro. Cuando se marca este segundo recuadro de selección, la planificación de este parámetro se distribuye. Consulte Distribuir configuración para obtener información sobre cómo distribuir selectivamente configuraciones. ¿Rearrancar o reiniciar portal? Alertador Recuadro de selección Activo al iniciar. Cada vez que se reinicia el dispositivo, el alertador se activa automáticamente. El reinicio de la interfaz gráfica de usuario no toma el valor Activo al iniciar. La distribución de configuración desde el Gestor central a las unidades gestionadas requiere que se rearranquen las unidades gestionadas para que tenga todo el efecto. El alertador se reinicia manualmente en las unidades gestionadas mediante el portal admin (consola de administración/alertador). Puesto que este reinicio no se puede realizar desde el Gestor central, reinicie las unidades gestionadas desde la consola de administración y obtenga el mismo efecto. Detección de anomalías Recuadro de selección Activo al iniciar. Cada vez que se reinicia el dispositivo, la detección de anomalías se activa automáticamente. El reinicio de la interfaz gráfica de usuario toma el valor Activo al iniciar. La distribución de configuración desde el Gestor central a las unidades gestionadas requiere reiniciar el portal en las unidades gestionadas para que se aplique completamente Inferencia de sesiones Recuadro de selección Activo al iniciar para iniciar Inferencia de sesiones cuando se inicie el dispositivo de Guardium. El reinicio de la interfaz gráfica de usuario toma el valor Activo al iniciar. La distribución de configuración desde el Gestor central a las unidades gestionadas requiere reiniciar el portal en las unidades gestionadas para que se aplique completamente Exportación de resultados/Copia de seguridad del sistema/Archivado de datos/Archivado de resultados/Exportación de datos La distribución de configuración desde el Gestor central a las unidades gestionadas se aplica sin reiniciar el portal en las unidades gestionadas Perfil global La distribución de la configuración desde el Gestor central a las unidades gestionadas se aplica sin reiniciar el portal en las unidades gestionadas (aunque si se utiliza una plantilla con otro nombre se aplicará sólo cuando se instale la política).

Control	Descripción
Registrar nuevo	Abre el panel Registro de unidades para registrar una unidad nueva para la gestión.
Estado de instalación de parches	La pantalla Estado de instalación de parches muestra, para cada unidad, las instalaciones fallidas y las discrepancias. Por ejemplo, si tiene un parche instalado sólo en algunas de las unidades, independientemente de si ha fallado en las otras unidades o si no se ha instalado.

Utilice el Gestor central para asignar alertas de correlación a unidades gestionadas individuales o a grupos de unidades gestionadas.

Esta nueva característica es para un entorno gestionado.

Permite que el gestor central asigne alertas de correlación a unidades gestionadas individuales o a grupos de unidades gestionadas. Puede asignarla a una unidad o a un grupo o bien puede excluirla de una unidad o de un grupo. También debe especificar si desea ejecutarla en el propio Gestor central. Los grupos utilizados son grupos de unidades gestionadas, los mismos tipos de grupos que se utilizan en la página Gestor central.

En el entorno gestionado, en el Gestor central, el Creador de alertas tiene una nueva sección para "Unidades gestionadas". En esta sección, especifique unidades gestionadas individuales o grupos de unidades gestionadas para incluirlos o excluirlos de una alerta. También puede especificar con un recuadro de selección si el propio Gestor central se incluye o excluye. El comportamiento predeterminado coincide con el comportamiento existente: las alertas se ejecutan en todas partes. Si especifica que las alertas no se deben ejecutar en todas partes, verifique que las alertas se ejecuten donde se especifique. La interfaz de usuario incluye cuatro opciones para incluir/excluir unidades individuales o grupos, así como recuadros de diálogos para seleccionar en la lista de grupos de gestión y, si así se desea, crear nuevos grupos de gestión o editar grupos de unidades gestionadas existentes.

En las unidades gestionadas individuales, el Creador de alertas no muestra ninguna sección sobre unidades gestionadas, sólo el Gestor central puede asignar alertas a unidades y grupos.

Si hay entradas en la tabla de alertas en una unidad gestionada determinada, se creará automáticamente un grupo generado por el sistema para excluir dicha unidad de cada alerta de la que se excluya. Esto ocurrirá cuando se inicien las alertas en esa unidad gestionada.

Los paneles de alerta de la página de detección de anomalías en la consola de administración se han utilizado para habilitar/inhabilitar localmente las alertas. Para esta característica, los paneles de alertas sólo aparecen en el Gestor central.

En las unidades gestionadas, ahora hay una tabla que muestra las alertas activas y si están habilitadas.

Tema principal: Utilización de las funciones de Gestión central

Instalación de políticas de seguridad en unidades gestionadas

Instale una política de seguridad en una unidad gestionada.

Acerca de esta tarea

Para instalar una política de seguridad en una unidad gestionada:

Procedimiento

1. Pulse Configuración > Herramientas y vistas > Instalación de política para abrir Políticas instaladas actualmente y el Instalador de políticas.
2. En la lista de políticas, seleccione la política que desee instalar.
3. En la lista, seleccione una acción de instalación. Después de seleccionar una acción de instalación, se le informará del éxito (o error) de cada instalación de política. Si una unidad seleccionada no está disponible (puede estar fuera de línea o un enlace podría estar inactivo), el Gestor central le informa de ese hecho. Continúa intentando instalar la nueva política durante un máximo de siete días (con la condición de que la unidad permanezca registrada para la gestión central).
4. En la lista de políticas, seleccione la política que desee instalar.
5. Las acciones de instalación disponibles incluyen los elementos siguientes:
    a. Instalar y modificar: Suprime todas las políticas instaladas e instala las políticas seleccionadas
    b. Instalar último: Instalación de la política seleccionada como la última de la secuencia; instalación de la política después de todas las políticas instaladas actualmente y que tienen la prioridad más baja
    c. Instalar primero: Instalación de la política seleccionada como la primera de la secuencia; instalación de la política antes de todas las políticas instaladas actualmente.

   Nota: Si instala una política desde el Gestor central, la selección de Ejecutar una vez ahora (y planificador) actualiza los grupos existentes en las políticas instaladas.

   Para cargar los cambios a las reglas, incluida la adición y resta de grupos, debe:

    a. Instalar inicialmente las políticas desde el recopilador, o bien
    b. Reinstalar las políticas desde el recopilador o Gestor central.

Tema principal: Utilización de las funciones de Gestión central

Gestión central de parches

Proporciona visibilidad y control sobre la instalación, el estado, y el historial de parches.

Acerca de esta tarea

Proporciona visibilidad y control sobre la instalación, el estado, y el historial de parches. En una Gestión central, proporciona una manera de instalar parches en unidades gestionadas desde el Gestor central.

Cuando se instala un parche, se puede especificar una solicitud de fecha y hora para indicar cuándo se instalará el parche. Si no se especifica ninguna fecha y hora o si se especifica ahora, la hora de la solicitud de instalación es inmediata.

Nota: Un parche que se ha instalado correctamente se puede volver a instalar. Este hecho es importante para los parches de proceso por lotes. Un aviso le informará de si el parche ya está instalado.

Inicie sesión en la interfaz gráfica de usuario de Guardium de la unidad que se gestionará como usuario de administración:

Procedimiento

1. Pulse Gestionar > Gestión central > Gestión central.
2. Seleccione las unidades que requieren el parche y pulse Distribución de parches
3. En la pantalla Distribución de parches, seleccione el parche que desea distribuir y pulse Instalar parche ahora o Planificar parche.
4. Para ver el estado de la instalación, pulse Gestionar > Gestión central > Gestión central y a continuación seleccione las unidades y pulse Estado de instalación de parches. La pantalla Estado de instalación de parches muestra, para cada unidad, las instalaciones fallidas y las discrepancias. Por ejemplo, si tiene un parche instalado sólo en algunas de las unidades, independientemente de si ha fallado en las otras unidades o si no se ha instalado. Para eliminar parches de la pantalla Distribución de parches, pulse el icono para suprimir (x roja) junto al parche. Esto no suprime el parche del directorio de distribución de parches en el dispositivo, pero lo eliminará de la pantalla.

Tema principal: Utilización de las funciones de Gestión central

Utilización de perfiles de configuración

Los perfiles de configuración le permiten definir valores de configuración y planificación desde un gestor central y distribuir dichos valores a grupos de unidades gestionadas sin alterar la configuración del propio gestor central.

Antes de empezar

Antes de crear y distribuir perfiles de configuración, verifique los requisitos previos siguientes:

- permitir la comunicación en el puerto 8447 entre el gestor central y sus unidades gestionadas
- el gestor central y las unidades gestionadas que recibirán configuraciones deben tener Guardium V10.1 o posterior.

Acerca de esta tarea

Los perfiles de configuración contienen dos tipos de información: uno o más conjuntos de valores de configuración y planificación, y una lista de grupos de unidades gestionadas que se actualizarán con los valores de configuración y planificación. Una vez definidos, los perfiles de configuración se pueden almacenar, modificar y reutilizar para distribuir conjuntos específicos de valores de configuración y planificación a grupos específicos de unidades gestionadas.

Los perfiles de configuración se definen independientemente de los valores locales en el gestor central. Esto le permite definir rápidamente los valores de configuración y desplegar estos valores en grupos de unidades gestionadas sin interrumpir la configuración del gestor central o configurar individualmente cada unidad gestionada.

Esta tarea describe cómo crear, distribuir y guardar un perfil de configuración.

Procedimiento

1. Vaya a Gestionar > Gestión central > Distribuir perfiles de configuración.
2. Pulse o seleccione un perfil existente para empezar a trabajar con un perfil de configuración.
3. En el panel Nombre y descripción, proporcione un nombre y, opcionalmente, una descripción para el perfil. Pulse Siguiente para continuar.
   Opcional: pulse el botón Roles para especificar los roles de seguridad que pueden utilizar el perfil de configuración.
4. En el panel Qué se va a distribuir, pulse para definir una nueva configuración, o seleccione una configuración existente y pulse para editar.
   a. En el menú Tipo de configuración, seleccione un tipo de configuración para añadir al perfil.
   b. Especifique los detalles de configuración y planificación para el tipo de configuración seleccionado. Para obtener más información sobre los valores de configuración, consulte la documentación del producto para el tipo de configuración que esté definiendo.
      Restricción: La distribución de valores de configuración de exportación de datos a un agregador no distribuirá valores de depuración. Los valores de depuración existentes en un agregador se conservarán. Los valores de depuración, incluidos los periodos de retención, se distribuirán a los valores de depuración existentes en los recopiladores y los sustituirán.
   c. Pulse Guardar para finalizar la edición de los detalles de configuración.
   Continúe añadiendo o editando configuraciones según se requiera. Pulse Siguiente para continuar.
5. En el panel Área de distribución, seleccione los grupos en la tabla Grupos de unidades gestionadas y utilice el icono para añadir los grupos a la tabla Grupos seleccionados. Pulse Siguiente para continuar.
   Nota: pulse para crear un nuevo grupo de unidades gestionadas o para editar un grupo existente. Los grupos de unidades gestionadas también se pueden definir y editar en Gestionar > Gestión central > Grupos de unidades gestionadas.
6. En el panel Distribuir configuraciones, pulse Ejecutar ahora para distribuir el perfil de configuración a los grupos seleccionados. Cuando el estado indique que la distribución se ha completado, pulse Siguiente para continuar.
7. En el panel Resultados de revisión, revise un resumen del proceso de distribución y sus resultados.
   Opcional: pulse Ejecutar registro para ver un registro detallado del proceso de distribución.
8. Pulse Guardar para guardar el perfil de configuración para su reutilización.

Qué hacer a continuación

Si necesita mover perfiles de configuración entre gestores centrales, utilice Gestionar > Gestión de datos > Exportación de definiciones y Gestionar > Gestión de datos > Importación de definiciones y seleccione Perfil de configuración en el menú Tipo.

Tema principal: Utilización de las funciones de Gestión central
Conceptos relacionados:
Agregación
Configuración del alertador
Exportar/Importar definiciones
Creación de alias IP-Nombre de host
Planificación

Distribuir configuración

Las configuraciones y sus planificaciones se pueden distribuir, ya sea todas o individualmente, entre el Gestor central y las unidades gestionadas.

Procedimiento

1. Seleccione las unidades gestionadas que reciben las configuraciones.
2. Pulse Distribuir configuraciones para visualizar la ventana Distribuir configuraciones.
3. Marque los recuadros de selección adecuados para las configuraciones que desee distribuir. Utilice el recuadro de selección en la cabecera para seleccionar todas las configuraciones.
4. Marque los recuadros de selección adecuados correspondientes a las planificaciones que desee distribuir. Utilice el recuadro de selección de la cabecera para seleccionar todas las planificaciones. Si una configuración no está planificada, no hay ningún recuadro de selección para ella y en su lugar se muestra n/d.
5. Pulse Distribuir para distribuir las configuraciones y planificaciones.
6. Opcional: Pulse Cancelar para terminar anormalmente la distribución.

Resultados

Si utiliza el mandato, Gestión central > Distribuir configuraciones > Perfil global, se distribuyen los valores siguientes:

- ACTIVATE_ALIASES
- CUSTOM_DB_MAX_SIZE
- CHECK_CONCURRENT_LOGIN
- HTML_BOTTOM_RIGHT
- HTML_BOTTOM_LEFT
- DISPLAY_LOGIN_MESSAGE
- LOGIN_MESSAGE
- CSV_DELIMETER
- FILTERING_ENABLED
- INCLUDE_CHILDREN_ON_FILTER
- SHOW_ALL_RECORDS
- ACCORDION_DISABLED
- SCHEDULER_RESTART_INTERVAL
- SCHEDULER_RESTART_WAIT_SHUTDOWN
- ESCALATE_TO_ALL
- MESSAGE_TEMPLATE

Tema principal: Utilización de las funciones de Gestión central

Distribuir configuración de autenticación

En lugar de configurar la autenticación en cada dispositivo individualmente, la autenticación de gestión central (Configurar autenticación) se puede configurar una sola vez en el gestor central y, a continuación, distribuir a todas las unidades gestionadas. De esta forma, la información se especifica una única vez y se aplica a algunas o a todas las unidades; algunas de las unidades pueden tener un tipo distinto de autenticación.

Procedimiento

1. Asegúrese de que la autenticación (Configurar autenticación) se realice en el gestor central y en la unidad gestionada. De esta forma, si se utiliza la autenticación LDAP, asegúrese de que LDAP esté configurado en el gestor central y en la unidad gestionada.
2. Seleccione las unidades gestionadas para recibir la distribución de la autenticación de gestión central.
3. Pulse Distribuir configuración de autenticación para distribuir la configuración de autenticación a todas las unidades gestionadas seleccionadas.

Tema principal: Utilización de las funciones de Gestión central

Redundancia de la Gestión central

Utilice Redundancia de la Gestión central o Gestor central secundario para configurar un Gestor central secundario o de copia de seguridad en caso de que el Gestor central primario deje de estar disponible.

La redundancia del Gestor central permite lo siguiente:

1. Gestor central secundario: el enlace Convertir en CM primario estará disponible después de que el Gestor central primario pierda la conexión.
2. Se mantendrán los diseños de usuario.
3. El usuario y los roles están en la copia de seguridad sincronizada y no se basarán en la sincronización de usuarios del portal.
4. Los roles de grupo de usuarios se mantendrán.
5. Se ha añadido una función de GuardAPI, make_primary_cm, para permitir pasar al Gestor central desde la CLI.
6. Los datos se mantienen de los procesos del Creador de procesos de auditoría después de pasar del Gestor central primario al Gestor central secundario.
7. La copia de seguridad de Gestión central incluye todas las definiciones (informes, consultas, alertas, políticas, procesos de auditoría, etc.), usuarios y roles que incluía anteriormente.
8. Incluye las planificaciones para informes empresariales, informes distribuidos y LDAP.
9. Incluye planificaciones para todos los procesos de auditoría, planificaciones y valores para procesos de gestión de datos, como por ejemplo archivado, exportación, copia de seguridad e importación.
10. Incluye valores para Alertador y Remitente.

11. Se incluyen las personalizaciones de la interfaz gráfica del usuario, las clases personalizadas y los controladores JDBC subidos del usuario.

Nota: No se incluyen los datos, ya sean datos recopilados, resultados de auditoría y datos de tablas personalizadas.
Nota:

Para listar el estado de cm_sync_file(s) en el Gestor central secundario, utilice el mandato de CLI show local_cm_sync_file. Para listar el valor de IP del Gestor central secundario para cada unidad gestionada, utilice el mandato GuardAPI, grdapi show_backup_cm_ip (este mandato de API sólo se puede ejecutar en un Gestor central).

Nota: Sustitución por anomalía con equilibrio de carga del Gestor central: tras la sustitución por anomalía, si las nuevas unidades gestionadas se conectan y a continuación se desconectan inmediatamente, no se enviará el DB_USER correcto hasta que se reciba el mensaje de sustitución por anomalía.

Realice estos pasos en el despliegue o servidores secundarios y pruebe. Si el resultado es correcto, realice estos pasos en los servidores de Guardium primarios o activos.

Instale los parches en el Gestor central

1. En el Gestor central primario actualmente, inicie sesión como CLI.
2. Instale los parches con el siguiente mandato de CLI, store system patch install scp
3. Este mandato de CLI copiará los archivos en el servidor de Guardium y le proporcionará la capacidad de instalarlos.
4. Vea cómo se instalan estos parches con el siguiente mandato de CLI, show system patch install
5. Espere hasta que el estado del parche muestre “DONE: Patch installation Succeeded.” para ambos parches.

Instale los parches en el Gestor central secundario

1. Inicie sesión como administrador en la interfaz gráfica de usuario primaria actualmente.
2. Seleccione Configuración > Herramientas y vistas y a continuación seleccione Gestor central.
3. Pulse los recuadros de selección de la unidad gestionada del Gestor central secundario SÓLO en el Gestor central.
4. Pulse Distribución de parches e instale todos los parches que acaba de instalar en el Gestor central primario.

Ejemplo de instalación de un parche

1. Pulse Distribución de parches.
2. Pulse Instalar parche ahora.
3. Espere unos 15 minutos para asegurarse de que el parche está instalado en todos los servidores gestionados.
4. Para verificarlo, inicie sesión como CLI en el Gestor central secundario y ejecute el mandato de CLI show system patch install desde el servidor de Gestor central secundario.

Instale los parches en todos los demás servidores gestionados (pasos opcionales)

1. Repita los pasos anteriores para instalar los parches en todos los servidores gestionados.
2. Verifique que todos los parches se hayan instalado antes de pasar al procedimiento siguiente.

Cuando se hayan instalado todos los parches en el Gestor central y los servidores gestionados

1. Inicie sesión como administrador en el Gestor central primario actualmente.
2. Seleccione Configuración > Herramientas y vistas y a continuación seleccione Gestor central. Pulse Designar Gestor central (CM) secundario.
3. Seleccione el servidor de Gestor central secundario en la lista de Gestores centrales secundarios candidatos que se muestra.
4. Pulse Aplicar.
5. Espere unos dos minutos a que el Gestor central secundario se sincronice y a que el NUEVO archivo de Gestor central secundario se cree y copie en el Gestor central secundario.
6. Espere a que se realicen dos rondas completas de copias de seguridad (aproximadamente 1 hora) para dos archivos de sincronización de Gestor central secundario que se copiarán en el Gestor central secundario y a que se puedan visualizar en el separador Supervisión de Guardium - Informe Registro de agregación/archivado.
7. Seleccione Supervisión de Guardium y seleccione el informe Registro de agregación/archivado para ver el progreso de la creación del archivo de sincronización del Gestor central secundario.
8. Compruebe que se haya iniciado la copia de seguridad de actividad y que se haya creado el archivo cm_sync_file.tgz desde el informe Registro de agregación/archivado.
    a. Inicie sesión como administrador desde la interfaz gráfica de usuario.
    b. Seleccione el separador Supervisión de Guardium.
    c. Seleccione Informe de agregación/archivado.
    d. Busque Tipos de copia de seguridad.
9. Cuando se completa:
    a. Los archivos se han instalado en el Gestor central.
    b. Los parches se han instalado en el Gestor central secundario.
    c. Opcional: Los parches se han instalado en todas las demás unidades gestionadas.

d. Se han completado dos archivos de sincronización de Gestor central secundario (consulte el archivo Registro de agregación/archivado en el separador Supervisión de Guardium).

e. Los pasos siguientes describen el proceso de conversión del Gestor central primario actual y sus nodos gestionados al Gestor central secundario.

Nota:

- IMPORTANTE: Espere aproximadamente una hora para asegurarse de que se hayan completado al menos DOS de los archivos de sincronización de Gestor central secundario que dan soporte al Gestor central secundario.
- La planificación de copias de seguridad de los archivos de sincronización del Gestor central secundario es de unos 30 minutos.
- El proceso se ejecutará en el Gestor central para crear un archivo de Gestor central secundario y copiará ese archivo en el directorio del Gestor central secundario.

Inicie el proceso del Gestor central secundario cuando se haya completado el proceso de los dos archivos de sincronización.

Concluya el servidor de Guardium del Gestor central primario

Si no tiene acceso para concluir el Gestor central primario, vaya directamente al Gestor central secundario e inicie sesión como administrador. (Seleccione Configuración > Herramientas y vistas y a continuación elija Gestión central y pulse Convertir en CM primario). Salte a la sección “Pasos para iniciar la configuración de Gestor central secundario a Gestor central primario” de este documento.

1. Espere unos cinco minutos y vuelva a iniciar sesión como administrador en la interfaz gráfica de usuario del Gestor central secundario.
2. Cuando haya concluido completamente el Gestor central primario, podrá continuar con el paso siguiente.

Nota:

Si ha iniciado sesión en el Gestor central primario y este se desactiva, recibirá un mensaje que indicará que la conexión ha excedido el tiempo de espera.

Pasos para iniciar la configuración del Gestor central secundario para convertirse en el Gestor central primario

El Gestor central secundario no responderá durante unos cinco minutos. Espere cinco minutos, inicie la sesión, y el enlace Convertir en CM primario estará disponible. El enlace está disponible cuando se inicia sesión como administrador en Configuración > Herramientas y vistas > Gestión central.

1. Cuando el servidor primario se desactive, recibirá un mensaje en el Gestor central secundario “No se ha podido conectar con el gestor remoto, considere la posibilidad de conmutar a (el nombre del Gestor central secundario)".
2. Si decide cambiarlo:
   a. Inicie sesión como administrador
   b. Seleccione Configuración > Herramientas y vistas.
   c. Pulse Convertir en CM primario. No pulse el enlace “Convertir en CM primario” más de una vez. Además, permanezca en esta pantalla y no seleccione nada más durante la ejecución de este proceso. Se creará un archivo de registro que puede visualizar para comprobar el progreso y la finalización del proceso. Tenga paciencia, ya que este proceso tardará algún tiempo en completarse. Como protección, si pulsa este botón más de una vez, no pasará nada con el proceso en ejecución en ese momento.
   d. Al cabo de unos segundos debería recibir un mensaje “¿Está seguro de que desea hacer que esta unidad sea el Gestor central (CM) primario? Pulse Aceptar.
   e. Unos segundos después recibirá un mensaje “Esto podría tardar algunos minutos”. El tiempo que tarda el Gestor central secundario en convertirse en Gestor central primario depende de la cantidad de datos de los que se haga copia de seguridad desde el archivo de sincronización del Gestor central secundario y del número de nodos gestionados que pasen al Gestor central secundario que se convertirán en Gestor central primario. Pulse Aceptar.

      Tan pronto como pulse Aceptar, se creará un archivo de registro denominado load_secondary_cm_sync_file.log que le permitirá ver el progreso del cambio hasta que se complete el proceso de pasar al Gestor central secundario. Este archivo se puede visualizar desde la interfaz gráfica de usuario. Los pasos siguientes indican cómo ver este archivo de registro.
   f. El último mensaje tardará algún tiempo en aparecer en la pantalla. Será el último mensaje antes de que se complete el cambio a Gestor central secundario. El mensaje es “Se reiniciará ahora la interfaz gráfica de usuario. Intente volver a iniciar la sesión en unos minutos y el Gestor central secundario será ahora el Gestor central primario”. Pulse Aceptar.

      Espere unos minutos a que el Gestor central secundario se convierta en el Gestor central primario y a que todos los nodos gestionados completen el cambio al nuevo Gestor central primario.

Visualización del archivo de registro de progreso mientras se ejecuta el proceso de copia de seguridad del Gestor central

Mientras se ejecuta el proceso Convertir en CM primario, desde el Gestor central secundario puede hacer lo siguiente para ver el progreso de la conversión del Gestor central secundario en Gestor central primario.

Requisito previo: Para ver los archivos de registro, necesitará la IP del servidor al que está conectado.

1. Inicie sesión como CLI desde el servidor del Gestor central secundario desde una sesión Putty.exe
2. Desde la CLI, ejecute Fileserver <IP> “especifique su número de IP” 3600", por ejemplo: fileserver 9.70.32.122 3600
3. Desde la interfaz gráfica de usuario, especifique el valor: http://su_servidor.x.x.x.com (aparecerá en la pantalla de la CLI tras especificar el mandato, por ejemplo: http://joe.server.guardium.com (el nombre de servidor será el servidor del Gestor central secundario).

   Se abrirá la ventana Servidor de archivos en la interfaz de usuario para seleccionar el archivo. Seleccione los registros Sqlguard.
4. Seleccione el archivo: load_secondary_cm_sync_file.log. (El archivo aparecerá en una lista de archivos del paso 3.) Esto le permitirá ver el progreso del cambio del Gestor central secundario a Gestor central primario.

   Localice el archivo de registro para verlo

El proceso de copia de seguridad del Gestor central se completa cuando ve esta línea en load_secondary_cm_sync_file.log

Importación de la información de sincronización del Gestor central - HECHO

5. Espere aproximadamente 10 minutos a que todas las unidades gestionadas pasen a estar disponibles para el nuevo Gestor central primario.

Cuando el Gestor central secundario se convierte en el Gestor central primario y el servidor del Gestor central secundario gestiona todos los nodos gestionados

Puede activar el anterior servidor del Gestor central. Cuando esté activo y en ejecución, realice los pasos siguientes para añadirlo al servidor del Gestor central secundario.

1. Rearranque el Gestor central primario.
2. Una vez que el servidor esté activo, inicie sesión como CLI.
3. Suprima el tipo de unidad de gestor, especificando delete unit type manager.
4. Cuando se complete, obtendrá un mensaje de la CLI conforme se ha realizado correctamente.
5. MUY IMPORTANTE: Espere unos cinco minutos a que la interfaz gráfica de usuario se reinicie completamente, incluso después de que el tipo de unidad suprimida muestre un mensaje que indique que la supresión se ha realizado correctamente y del mensaje de reinicio de la interfaz gráfica de usuario.
6. Espere cinco minutos e inicie sesión en el nuevo Gestor central primario para registrar el Gestor central anterior como una unidad gestionada.
7. Inicie sesión como administrador en el nuevo Gestor central primario.
8. Seleccione Configuración > Herramientas y vistas > Gestión central.
9. Pulse Registrar nuevo.
10. Especifique la IP del Gestor central primario anterior que acaba de rearrancar.
11. Especifique 8443 como puerto.
12. Pulse Guardar. (IMPORTANTE: Tenga paciencia, no pulse este botón dos veces).
13. Espere un minuto a que se registre el Gestor central primario anterior.
14. Haga del Gestor central primario anterior un nuevo Gestor central secundario.
15. Pulse Designar Gestor central (CM) secundario.
16. Pulse Servidor del Gestor central (CM) primario anterior.
17. Pulse Aplicar.
18. El servidor del Gestor central primario anterior es AHORA el nuevo servidor del Gestor central secundario.
19. Renueve la pantalla Gestión central para ver el nuevo tipo de unidad Gestor central secundario definido.
20. Esta tarea se ha completado.

Datos de informe después de que se complete el proceso de Gestor central (CM) secundario

Cuando se completa el proceso de Gestor central (CM) secundario, faltan los datos siguientes. Esto está relacionado con sólo el "primer" cambio de Gestor central primario a Gestor central secundario.

Datos que faltan:

1. Resultados del proceso de auditoría
2. Datos de tabla personalizada
3. Datos de informes personalizados
4. Resultados de VA
5. Resultados de clasificador
6. Resultados de DSD
7. Resultados de CAS
8. Datos de despensa de datos
9. Datos recopilados
10. Datos de titularidad

Los informes se volverán a llenar cuando ejecute de nuevo estos informes en el nuevo Gestor central primario. Si vuelve a cambiar al Gestor central primario anterior, se presentarán los datos de estos informes.

Tema principal: Utilización de las funciones de Gestión central

Centro de investigación

El centro de investigación es una extensión de los servidores de agregación. Los usuarios de investigación (una vez definidos) pueden restaurar datos y resultados de las fechas históricas seleccionadas y realizar investigación forense. Una vez que se han restaurado los días (fechas), los usuarios de investigación pueden definir y ver informes utilizando la interfaz de usuario estándar de Guardium, sólo en el ámbito de las fechas investigadas.

Cada dispositivo de Guardium mantiene un catálogo de todos los datos y resultados archivados. El catálogo contiene información sobre el archivado, su ubicación y las credenciales para acceder a ellos. El catálogo se exporta desde los recopiladores y se fusiona en un catálogo completo en el servidor de agregación como parte del proceso de agregación. Con el catálogo en su lugar, los usuarios de investigación ahora pueden seleccionar las fechas que deseen para la restauración y estas fechas se subirán automáticamente al centro de investigación y se fusionarán en la vista de ese usuario de investigación. Además de fusionar los catálogos de los recopiladores mediante el servidor de agregación, también es posible exportar e importar catálogos desde Configuración > Herramientas y vistas.

Usuarios y roles

En un servidor de agregación de Guardium hay un rol de investigación especial (inv). Los usuarios con el rol inv pueden realizar investigaciones forenses sobre datos históricos.

Un usuario de investigación utiliza principalmente las mismas definiciones de informe y consulta que cualquier otro usuario. La mayor diferencia es que el usuario de investigación sólo ve los datos seleccionados para su base de datos de investigación (se pueden configurar varios investigadores para compartir una base de datos INV). Los datos seleccionados pueden restaurarse del archivado o visualizarse de la base de datos actual en el caso de datos que todavía no se hayan depurado. Un usuario de investigación también puede restaurar resultados del proceso de auditoría archivados y visualizarlos.

Precaución: el rol inv es un rol especial que hará que el usuario esté conectado a una base de datos interna aparte sólo de investigación. Se debe combinar con el rol user y en general es incompatible con todos los demás roles.

Nota: Para configurar correctamente un usuario de investigación, el apellido del usuario debe establecerse en el nombre de las tres bases de datos de investigación, INV_1, INV_2 o INV_3 (con distinción de mayúsculas y minúsculas).

Cuando se crea un usuario de investigación, se sugiere que el nombre del usuario se corresponda con el nombre la base de datos de investigación que utilizará o que tenga alguna representación que la indique. Por ejemplo, si un usuario utilizará la base de datos INV_1, el nombre del usuario podría ser john1 o inv1.

Nota: El botón Ejecutar un proceso de auditoría ad hoc está disponible en todas las pantallas de informe para todos los usuarios, excepto para el usuario de investigación (INV).

Proceso de auditoría y rol INV

Si el usuario es INV, el buscador de procesos de auditoría mostrará los procesos de auditoría según los roles y la propiedad, pero sólo mostrará Clonar o Nuevo para todos los procesos de auditoría que no sean propiedad de INV.

Si el usuario es INV, la pantalla del menú de definición del proceso de auditoría permitirá lo siguiente:

- Sólo se permite a los usuarios de investigación y/o a direcciones de correo electrónico específicas como receptores (no se permite como receptores usuarios, grupos, ni roles normales que no sean INV).
- El botón Sucesos y columnas adicionales en una tarea de auditoría de informe guardada está siempre inhabilitado. No se puede especificar ninguna automatización de API.
- No se puede especificar ninguna planificación. En el proceso de auditoría en INV, los datos sólo se pueden ejecutar manualmente utilizando el botón Ejecutar ahora.
- Sólo se permiten tareas de auditoría de tipo Informe.
- Activo está inhabilitado, los campos Conservar días y Conservar ejecuciones están inhabilitados.

Si el usuario no es INV, el buscador de procesos de auditoría no mostrará los procesos de auditoría que sean propiedad del usuario de investigación (independientemente de los roles asignados).

Cuando se ha ejecutado un proceso de auditoría en datos INV, se añaden al título del resultado las palabras Ejecutado en centro de investigación por, seguido del nombre del usuario INV.

Se adjunta un comentario a los resultados que especifica las fechas y los hosts de origen de los datos montados en la base de datos de investigación en el momento de la ejecución.

Los resultados se pueden visualizar desde el Creador de procesos de auditoría o para la lista de navegación de resultados.

Los resultados de auditorías ejecutadas en el centro de investigación no se pueden archivar y se descartarán cuando se descarten los datos de investigación.

Contexto de investigación

El centro de investigación de Guardium da soporte a tres periodos de investigación simultáneos, denominados INV_1, INV_2 e INV_3, cada uno de los cuales puede contener datos históricos y proporciona los medios para la investigación forense de ese periodo. Cuando se crea un usuario de investigación, el apellido del usuario debe ser INV_1, INV_2 o INV_3, para asociar ese usuario a una de las bases de datos de investigación. Cuando se inicia sesión en el centro de investigación (utilizando uno de los usuarios de investigación), una etiqueta especifica el periodo de investigación seleccionado.

Interfaz gráfica de usuario

Un usuario con el rol de investigación verá dos separadores adicionales que son específicos del centro de investigación.

- El separador Auditoría proporciona acceso a los resultados del proceso de auditoría
- El separador Gestión de volumen permite al usuario establecer o modificar el periodo de investigación, seleccionar los resultados del proceso de auditoría para restaurar y descartar datos al final de una investigación.

Utilización del centro de investigación

- Restaurar un periodo de investigación
- Restaurar resultados de auditoría
- Ver registro de restauración
- Ver resultados de auditoría restaurados

Restaurar un periodo de investigación

Después de iniciar sesión en la interfaz de Guardium como usuario con el rol inv:

1. Pulse Gestionar > Gestión de datos > Restaurar datos para abrir Criterio de búsqueda de restaurar datos.
2. C
3. Pulse Restaurar datos para abrir el panel Datos restaurados. Si se ha realizado una restauración anterior, este panel mostrará los periodos de datos montados actualmente que se están utilizando. En este punto, puede pulsar Descartar datos para desmontar los periodos de datos montados anteriormente.
4. Pulse Volver a seleccionar el periodo de investigación para abrir el panel Criterio de búsqueda de restaurar datos.
5. Especifique la fecha de inicio en el recuadro Desde: para la fecha de inicio del periodo de tiempo que desea buscar.
6. Especifique la fecha de finalización en el recuadro Hasta: para la fecha de finalización del periodo que desea buscar.
7. Opcionalmente, especifique un nombre de host como ayuda para filtrar el conjunto de resultados con el nombre de host
8. Pulse Buscar para ver el conjunto de resultados. Esto buscará en el catálogo todos los archivos que coincidan con los criterios de búsqueda.
9. En el conjunto de resultados generado, marque el recuadro de selección de los periodos que desee restaurar. También puede pulsar Seleccionar todo o Deseleccionar todo para agilizar el proceso de selección.
10. Pulse Restaurar para restaurar los periodos seleccionados. En función del número de periodos que restaure, y de si los conjuntos de datos son locales al sistema, el proceso de restauración podría requerir mucho tiempo.
11. Puede supervisar el progreso del proceso de restauración en el panel Ver registro de restauración.

Nota: Los datos de cualquier día restaurados al centro de investigación que se encuentren dentro del periodo de fusión se fusionarán también con la base de datos de la aplicación de Guardium y los usuarios que no sean inv los visualizarán.

Restaurar resultados de auditoría

Un recuadro de selección en el Creador de procesos de auditoría permite especificar si los resultados de un proceso se deben archivar o no. Sólo se archivarán los resultados de los procesos marcados para el archivado para los que todos los firmantes han firmado. Los resultados de una ejecución específica se empaquetan, comprimen y almacenan, la ubicación se registra en el catálogo y los resultados de auditoría de restauración los utilizan para la selección y restauración. Los resultados archivados del proceso de auditoría de Guardium se pueden restaurar en un centro de investigación y contienen los resultados, la vista y los seguimientos de aprobación, así como los comentarios asociados con estos resultados.

Después de iniciar sesión en la interfaz de Guardium como usuario con el rol inv:

1. Pulse el separador Gestión de volumen.
2. Pulse Restauración de resultados de auditoría para abrir el panel Resultados restaurados. Si se ha realizado una restauración anterior, este panel mostrará los resultados restaurados actualmente que se estén utilizando. En este punto, puede pulsar Descartar datos para desmontar todos los resultados montados anteriormente.
3. Pulse Restauración de resultados de auditoría para abrir el panel Criterios de búsqueda de restauración de resultados.
4. Especifique la fecha de inicio en el recuadro Desde: para la fecha de inicio del periodo de tiempo que desea buscar.
5. Especifique la fecha de finalización en el recuadro Hasta: para la fecha de finalización del periodo de tiempo final que desea buscar.
6. Opcionalmente, especifique Nombre de host, Proceso de auditoría o Núm. ejecución como ayuda para filtrar el conjunto de resultados.
7. Pulse Buscar para ver el conjunto de resultados.
8. En el conjunto de resultados generado, marque el recuadro o recuadros de selección de los resultados que desea restaurar. También puede pulsar Seleccionar todo o Deseleccionar todo para agilizar el proceso de selección.
9. Pulse Restaurar para restaurar los resultados seleccionados. En función del número de resultados que se deban restaurar y de si los conjuntos de datos son locales para el sistema, el proceso de restauración podría tardar mucho tiempo.
10. Puede supervisar el progreso del proceso de restauración en Ver registro de restauración.

Ver registro de restauración

El registro de restauración proporciona una vista del archivado/restauración de intentos de restauración pasados y actuales, filtrada para el usuario con la sesión iniciada en ese momento. Este registro permite al usuario validar una restauración correcta de resultados de auditoría y datos.

Después de iniciar sesión en la interfaz de Guardium como usuario con el rol inv, pulse Registro de restauración para abrir Registro de mi restauración. En este panel podrá ver el estado de todos los intentos de restauración.

Ver resultados de auditoría restaurados

Después de iniciar sesión en la interfaz de Guardium como usuario con el rol inv:

1. Pulse el separador Auditoría.
2. Pulse el enlace Navegación de resultados para abrir el panel Buscador de procesos de auditoría.
3. En la lista desplegable (si hay procesos de auditoría), seleccione un proceso.
4. Pulse Ver para abrir otra ventana y ver los informes disponibles para los resultados de auditoría.

Tema principal: Agregación y gestión central

Gestión del sistema Guardium

Las tareas de gestión incluyen la supervisión del estado del sistema y la gestión de artefactos como, por ejemplo, grupos, dominios y notificaciones.

- Administración de Guardium
  Los administradores de Guardium realizan diversas tareas de administración y mantenimiento.
- Certificados
  Compruebe los certificados periódicamente para evitar la pérdida de funciones. Utilice los mandatos de CLI para obtener e instalar nuevos certificados.
- Nivel de utilización de unidad
  Utilice los informes de utilización de unidad para identificar los sistemas infrautilizados y sobreutilizados en el entorno de Guardium.
- Subidas de cliente
  Database Activity Monitor Content Subscription (denominado anteriormente Database Protection Subscription Service) da soporte al mantenimiento de pruebas de asesoramiento predefinidas, pruebas basadas en SQL, CVE, APAR y grupos como por ejemplo versiones y parches de base de datos.
- Panel Estado de Servicios
  El panel Estado de servicios es una ubicación centralizada donde comprobar el estado de los servicios como, por ejemplo, CAS o el alertador, y, si es necesario, investigar con mayor detalle cada servicio. Abra el panel Estado de servicios pulsando Configuración > Herramientas y Vistas > Estado de servicios. Cada vez que se abre el panel Estado de servicios, se renueva el estado de cada servicio.

- Archivado, depuración y restauración
  Las operaciones de archivado y depuración se deberían ejecutar de forma planificada. Utilice Archivado de datos y Archivado de resultados para almacenar la información capturada y la información para auditoría. Copia de seguridad y archivado Amazon S3 en Guardium también aparece al final de este tema.
- Catálogo de Guardium
  Cuando archiva datos del sistema Guardium, el catálogo de Guardium realiza un seguimiento de dónde se envía cada archivo de archivado, para que se pueda recuperar y restaurar.
- Cómo gestionar la copia de seguridad y el archivado
  Establezca prácticas de retención de datos; controle el volumen de actividad; gestione la planificación del archivado y la depuración de datos y haga copias de seguridad mensuales.
- Exportación de resultados (CSV, CEF, PDF)
  Los procesos de flujo de trabajo pueden crear archivos CSV, CEF y PDF. Esta función exporta todos estos tipos de archivo que se encuentran en el sistema Guardium.
- Exportar/Importar definiciones
  Si tiene varios sistemas con requisitos idénticos o similares, y no utiliza Gestión central, puede definir los componentes que necesita en un sistema y exportar esas definiciones en otros sistemas, siempre y cuando esos sistemas tengan el mismo nivel de release de software.
- Interfaz distribuida
  Utilice esta pantalla de configuración para definir la interfaz distribuida y subir el archivo de almacenamiento intermedio de protocolo (.proto) a la base de datos DIST_INT.
- Gestionar clases personalizadas
  Suba y mantenga clases personalizadas utilizadas en alertas o evaluaciones. Gestione las clases personalizadas pulsando Configuración > Clases personalizadas.
- Subida de un archivo de claves
  En condiciones excepcionales se debe subir un archivo de claves de Microsoft SQL Server al sistema Guardium para supervisar el tráfico cifrado de SQL Server.
- Claves públicas SSH
  Utilice esta información para crear, modificar o eliminar una clave pública SSH.
- Cómo instalar un certificado de dispositivo para evitar un reto de certificado SSL del navegador
  Utilice los mandatos de CLI de IBM Security Guardium para crear una solicitud de firma de certificado (CSR) e instalar certificados de servidor, autoridad emisora de certificados o vías de acceso de confianza en el sistema Guardium.
- Autosupervisión
  La solución Guardium se supervisa a sí misma para minimizar las interrupciones y corregir automáticamente los problemas siempre que sea posible.
- Grupos
  La utilización de grupos facilita la creación y gestión de definiciones de clasificador, política y consulta, así como el despliegue de actualización en los clientes de GIM y S-TAP. En lugar de definir repetidamente un grupo de objetos de datos para una política de acceso, ponga los objetos en un grupo para gestionarlos fácilmente.
- Roles de seguridad
  Se utilizan roles de seguridad para otorgar acceso a los datos (grupos, consultas, informes, etc.) y otorgar acceso a aplicaciones (Creador de grupos, Creador de informes, Creador de políticas, CAS, Asesoramientos de seguridad, etc).
- Notificaciones
  Utilice el Alertador y el Creador de alertas para crear notificaciones. Cuando se requieran notificaciones por correo electrónico u otras para acciones de alerta, siga este procedimiento para cada tipo de notificación que se vaya a definir.
- Cómo crear una alerta en tiempo real
  Envíe una alerta en tiempo real al administrador de base de datos siempre que haya más de tres inicios de sesión fallidos para el mismo usuario en un plazo de cinco minutos.
- Administración de clase de alerta personalizada
  Utilice una clase de alerta personalizada para enviar alertas a un destinatario personalizado. Suba la clase personalizada y, a continuación, utilice el Creador de alertas para designar la clase personalizada como un receptor de notificaciones de alerta.
- Alertas predefinidas
  Tabla que describe las alertas predefinidas que se encuentran en el Creador de alertas.
- Planificación
  El planificador de uso general se utiliza para planificar muchos tipos diferentes de tareas (archivado, agregación, automatización de flujo de trabajo, etc.) .
- Alias
  Cree sinónimos para valores de datos u objetos que se utilizarán en informes o consultas.
- Fechas e indicaciones de fecha y hora
  Utilice una herramienta de calendario para seleccionar una fecha exacta, y un selector de fecha relativa para seleccionar una fecha relativa a la hora actual.
- Periodos de tiempo
  Utilice el Creador de periodos de tiempo para crear periodos de tiempo que se pueden utilizar para reglas de política y condiciones de consulta.
- Periodos de tiempo
  Las reglas de política y las condiciones de consulta pueden probar los sucesos que se producen (o no) durante los periodos de tiempo definidos por el usuario.
- Comentarios
  Los comentarios se aplican a definiciones y a resultados de proceso de flujo de trabajo.
- Cómo instalar parches
  Instalar un único parche o varios parches como un proceso en segundo plano.
- Mantenimiento de soporte
  La característica Mantenimiento de soporte está protegida con contraseña y sólo se puede utilizar tal como lo indique el soporte técnico. Si requiere información adicional, póngase en contacto con el Soporte técnico.

Administración de Guardium

Los administradores de Guardium realizan diversas tareas de administración y mantenimiento.

Cualquier usuario asignado al rol admin se conoce como administrador de Guardium. No es lo mismo que la cuenta del usuario de administración.

Privilegios del rol admin

El rol admin de Guardium tiene privilegios que no se han asignado explícitamente a ese rol. Por ejemplo, cuando un usuario con el rol admin visualiza una lista de definiciones de conjunto de privacidad, se visualizan todos los conjuntos de privacidad definidos en el sistema Guardium y el usuario con el rol admin puede visualizar, modificar o suprimir cualquiera de estas definiciones. Cuando un usuario sin el rol admin accede a la lista de conjuntos de privacidad, ese usuario verá sólo los conjuntos de privacidad de los que es propietario (es decir, ha creado) y todos los conjuntos de privacidad que tienen asignado un rol de seguridad también se asignan a ese usuario.

Acceso al mandato de CLI diag

El uso del mandato de CLI diag requiere una contraseña adicional, que puede ser la contraseña de cualquier usuario con el rol admin.

Si está habilitado el bloqueo automático de cuenta (una característica que bloquea una cuenta de usuario tras un número especificado de errores de inicio de sesión), la cuenta de usuario de administración puede quedar bloqueada tras un número de intentos fallidos de inicio de sesión. Si esto sucede, utilice el mandato de CLI unlock admin para desbloquearla.

Nota: El gestor de acceso (accessmgr) puede desbloquear las cuentas desde el Explorador de usuarios. Abra el Explorador de usuarios pulsando Acceso > Gestión de acceso > Explorador de usuarios.

Privilegios del usuario de administración

El usuario de administración tiene privilegios adicionales que no se otorgan al rol admin, de la forma siguiente:

- Acceso a las listas de tareas pendientes de todos los usuarios
- Propietario de las definiciones importadas
- Funciones de gestión de acceso

Poderes de lista de tareas pendientes del usuario de administración

La Lista de tareas pendientes es una característica de automatización de flujo de trabajo que controla la distribución de los resultados de proceso de auditoría a los usuarios. El usuario de administración tiene responsabilidades y privilegios especiales en esta área. Si una cuenta de usuario está inhabilitada, todos los resultados de proceso de auditoría para ese usuario se reasignarán automáticamente al usuario de administración. Si por alguna otra razón un usuario no está disponible, los resultados de proceso de auditoría se pueden instalar en la lista de tareas pendientes de ese usuario, es decir, a la espera de aprobación antes de que se suministren al siguiente receptor de resultados. El usuario de administración puede abrir la lista de tareas de cualquier usuario y realizar las acciones disponibles para ese usuario. Cuando el usuario de administración realiza alguna acción en la lista de tareas pendientes de otro usuario, este hecho se indica en el registro de actividad del proceso de auditoría, por ejemplo, `El usuario admin ha aprobado resultados en nombre del usuario x`.

Propiedad de una definición importada

Cuando se exportan definiciones, se eliminan todos los roles y el propietario se cambia al usuario de administración. Esta es la única manera de controlar cómo se utilizará la definición en el sistema de importación.

Gestión de acceso y el administrador

Por motivos de seguridad, existe una separación de responsabilidades para el gestor de acceso y el administrador. Los usuarios de administración no pueden tener privilegios de gestor de acceso, ni viceversa.

La próxima vez que el usuario de administración inicie sesión tendrá disponible la funcionalidad de acceso. Esto es posible sólo para el usuario de administración (y no para otros usuarios que tengan el rol admin).

Nota:

El mismo usuario puede contener ambos roles como resultado de una situación heredada o de una actualización. Sin embargo, el uso actual no permitirá que se asignen los dos roles al mismo usuario.

En el pasado, cuando se actualizaba una unidad, el rol accessmgr se asignaba al usuario de administración, y el usuario accessmgr se inhabilitaba.

En esta situación, para configurar accessmgr y admin, inicie sesión como admin y habilite el usuario accessmgr y, a continuación, inicie sesión como accessmgr (la contraseña inicial predeterminada es `guardium`) y elimine el rol accessmgr del usuario admin.

Tema principal: Gestión del sistema Guardium

Certificados

Compruebe los certificados periódicamente para evitar la pérdida de funciones. Utilice los mandatos de CLI para obtener e instalar nuevos certificados.

Caducidad de certificado

Los certificados caducados resultarán en una pérdida de función. Ejecute el mandato show certificate warn_expire periódicamente para comprobar si hay certificados caducados. El mandato muestra los certificados que caducarán en el plazo de seis meses y los certificados que ya han caducado. La interfaz de usuario también le informará de los certificados que caducarán. Para ver un resumen de todos los certificados, ejecute el mandato show certificate summary.

Para obtener más información, consulte la lista completa de Mandatos de CLI de certificado.

Nuevos certificados

Para obtener un nuevo certificado, genere una solicitud firmada de certificado (CSR) y póngase en contacto con una autoridad emisora de certificados externa (CA), como VeriSign o Entrust. Guardium no proporciona servicios de autoridad emisora de certificados y no proporcionará sistemas con certificados distintos a los que se instalan de forma predeterminada. El formato del certificado debe estar en PEM e incluir delimitadores BEGIN y END. El certificado se puede pegar desde la consola o importar mediante uno de los protocolos de importación estándar.

Puede generar una solicitud de certificado firmado (CSR) con uno de los mandatos siguientes:

- create csr alias: Este mandato crea una solicitud de certificado con un alias.
- create csr gui: Este mandato crea una solicitud de certificado para Tomcat.
- create csr sniffer: Este mandato crea una solicitud de certificado para el sniffer.

Nota: No realice esta acción hasta que se hayan establecido los parámetros de configuración de red del sistema.
Para instalar un certificado nuevo mediante la interfaz de línea de mandatos, utilice uno de los siguientes mandatos:

- store certificate gim: Este mandato almacena los certificados de GIM en el almacén de claves.
- store certificate gui: Este mandato almacena los mandatos de tomcat en el almacén de claves.

- store certificate keystore: Este mandato solicita un alias de una sola palabra para identificar de forma exclusiva el certificado y almacenarlo en el almacén de claves.
- store certificate mysql: Este mandato almacena los certificados de cliente y servidor de mysql.
- store certificate stap: Este mandato almacena certificados de S-TAP.
- store certificate sniffer: Este mandato almacena certificados de sniffer.

Para instalar una nueva clave de certificado mediante la interfaz de línea de mandatos, utilice uno de los mandatos siguientes:

- store cert_key mysql: Este mandato almacena la clave de certificado de un cliente y servidor de mysql.
- store cert_key sniffer: Este mandato almacena la clave de certificado de sniffer.

Opciones backup y default

Puede optar por restaurar certificados y claves de certificados con el parámetro backup o default. Utilice el parámetro backup para restaurar un certificado al último certificado guardado. Utilice el parámetro default para restaurar un certificado al certificado original proporcionado por Guardium.

Cambios en los mandatos

Algunos mandatos de certificado han cambiado.

- csr es ahora create csr gui.
- create system csr es ahora create csr sniffer.
- restore keystore es ahora restore certificate keystore backup.
- restore system-certificate es ahora restore certificate sniffer default.
- show system certificate es ahora show certificate sniffer.
- store system certificate es ahora store certificate sniffer.
- store trusted certificate es ahora store certificate keystore.
- store certificate console es ahora store certificate gui.

Mandatos nuevos

Los mandatos siguientes están disponibles para su uso.

- create csr alias
- restore certificate keystore default
- restore certificate sniffer backup
- show certificate all
- show certificate gim
- show certificate gui
- show certificate keystore alias
- show certificate keystore all
- show certificate mysql client
- show certificate mysql server
- show certificate summary
- show certificate warn_expired

Mandatos en desuso

Los mandatos siguientes están en desuso.

- csr
- store certificate console
- store system key
- show system key
- store system certificate
- show system certificate

Lista completa de mandatos

Utilice los mandatos siguientes para crear, restaurar, mostrar o almacenar certificados.

- create csr gui
- create csr alias
- create csr sniffer
- restore certificate keystore default
- restore certificate keystore backup
- restore certificate sniffer backup
- restore certificate sniffer default
- show certificate all
- show certificate gim
- show certificate gui
- show certificate keystore alias
- show certificate keystore all
- show certificate mysql client
- show certificate mysql server
- show certificate sniffer
- show certificate summary
- show certificate warn_expired
- store certificate sniffer
- store certificate gui

Nivel de utilización de unidad

Utilice los informes de utilización de unidad para identificar los sistemas infrautilizados y sobreutilizados en el entorno de Guardium.

Abra los informes de utilización de unidad pulsando Gestionar > Informes > Utilización de unidad y, a continuación, seleccionando uno de los informes.

Los informes de utilización de unidad incluyen lo siguiente:

- Supervisor de uso de almacenamiento intermedio
- Rastreador de CPU
- Supervisor de uso de almacenamiento intermedio de empresa
- Utilización de unidad

Parámetros de utilización

Se realiza el promedio de la mayoría de los parámetros para una unidad específica durante un rango de tiempo específico. El número de reinicios es un recuento del número de reinicios del sniffer durante un rango de tiempo específico según los distintos PID.

Los parámetros soportados son:

- Número de reinicios
- Memoria del sniffer
- Porcentaje de memoria de MySQL
- Espacio de almacenamiento intermedio libre
- Cola de analizador
- Cola de registrador
  Restricción: Existe un límite de 500 SQL en la cola del registrador. Si más de 500 SQL intentan llenar esta cola al mismo tiempo, cualquier SQL adicional por encima del límite de la cola registrará `RA=-1`.
- Uso de disco de MySQL
- Carga de CPU del sistema
- Uso del disco Var del sistema
- Número de solicitudes
- Número de SQL completo
- Número de excepciones
- Número de infracciones de política
- Búsqueda rápida del uso del disco
- Búsqueda rápida del número de documentos
- Solicitudes de proceso flat log

Umbrales

Para cada parámetro, hay dos umbrales definidos que separan tres niveles de utilización: Baja, Media y Alta.

Niveles de utilización:

- Baja: el valor es menor que Umbral1
- Media: el valor es mayor que Umbral1, y menor que Umbral2
- Alta: el valor es mayor que Umbral2

También hay un nivel de utilización global para cada unidad. Para cada periodo de tiempo, este nivel es el nivel más alto para todos los niveles durante ese periodo.

Creación de informes

Vea los informes de utilidad de unidad disponibles pulsando Gestionar > Informes > Utilización de unidad.

La opción de seguimiento de Niveles de utilización de unidad le permite crear consultas e informes personalizados.

Se recomienda utilizar alias cuando se utilicen datos de utilización de unidad en informes personalizados y definidos. De lo contrario, los niveles de utilización se visualizarán como números: 1, 2, 3, en lugar de Baja, Media, Alta.

La lista de atributos incluye:

- Nombre de host
- Inicio de periodo
- Número de reinicios
- Nivel de número de reinicios
- Memoria del sniffer
- Nivel de memoria de sniffer
- Porcentaje de memoria de MySQL
- Porcentaje de nivel de memoria de MySQL
- Espacio de almacenamiento intermedio libre
- Nivel de espacio de almacenamiento intermedio libre
- Cola de analizador
- Nivel de cola de analizador
- Cola de registrador
- Nivel de cola de registrador
- Uso de disco de MySQL
- Nivel de uso de disco de MySQL
- Carga de CPU del sistema
- Nivel de carga de CPU del sistema

- Uso del disco Var del sistema
- Nivel de uso del disco Var del sistema
- Nivel de utilización de unidad global
- Número de solicitudes
- Nivel de número de solicitudes
- Número de SQL completo
- Nivel de número de SQL completo
- Número de excepciones
- Nivel de número de excepciones
- Número de infracciones de política
- Nivel de número de infracciones de política
- Número de solicitudes de Flat Log
- Nivel de número de solicitudes de Flat Log

Nota: Cada parámetro tiene un valor y un nivel que se calcula según el valor y los umbrales.

Información de rendimiento disponible en Utilización de unidad

Se recopilan datos de rendimiento en cada unidad de recopilador. El gestor central consolida todos los datos de rendimiento y crea una tabla personalizada empresarial que se añade a los informes de utilización predefinidos.

Información de rendimiento recopilada:

- Número de solicitudes (para el periodo) (de la instancia de construcción)
- Número de SQL completos (para el periodo) (del texto de construcción)
- Número de excepciones
- Número de infracciones de política

De forma predeterminada, la información de rendimiento se recopila cada hora.

Mandatos de GuardAPI y CLI de Utilización de unidad

API de Guard:

- listUtilizationThresholds

  updateUtilizationThresholds

  reset_unit_utilization

Mandatos de CLI:

- store monitor gdm_statistics
- show monitor gdm_statistics

- Configuración del proceso de datos de utilización de unidad
  Este procedimiento describe cómo configurar sistemas Guardium para procesar y visualizar datos de utilización de unidad.

Tema principal: Gestión del sistema Guardium

Configuración del proceso de datos de utilización de unidad

Este procedimiento describe cómo configurar sistemas Guardium para procesar y visualizar datos de utilización de unidad.

Acerca de esta tarea

Para un entorno gestionado centralmente, la visualización de información de utilización de unidad requiere la planificación de dos procesos en el gestor central: la subida de datos para el supervisor de uso de almacenamiento intermedio del gestor central y el proceso de los datos de utilización de unidad.

En el caso de un sistema autónomo, la visualización de la información de utilización de unidad sólo requiere la planificación del proceso de los datos de utilización de la unidad. No es necesario planificar la subida de datos para un supervisor de uso de almacenamiento intermedio de gestor cuando se trabaja con un sistema autónomo.

Procedimiento

1. Para un entorno gestionado centralmente, defina una planificación en el gestor central para la subida de los datos del supervisor de uso de almacenamiento intermedio del gestor central.
   a. Vaya a Informes > Herramientas de configuración de informes > Generador de tablas personalizadas.
   b. En la pantalla Tablas personalizadas, seleccione Supervisor de uso de almacenamiento intermedio de CM y pulse Subir datos para continuar.
   c. En la pantalla Subir datos, pulse Modificar planificación para definir una planificación para subir los datos del supervisor de uso de almacenamiento intermedio de gestor central. Pulse Guardar después de definir una planificación y, a continuación, pulse Atrás para volver a la pantalla Subir datos. Un punto de partida razonable para muchos despliegues es planificar el proceso para que se ejecute una vez cada hora, pero es posible que desee ajustar el intervalo según los recursos disponibles o las necesidades de datos.
   Importante: Para asegurarse de que los datos más recientes están disponibles para los informes de utilización de unidad, defina una planificación que procese los datos del supervisor de uso de almacenamiento intermedio antes de procesar los datos de utilización de la unidad. Además, los datos del supervisor de uso de almacenamiento intermedio no deben planificarse para ejecutarse exactamente a la hora.
   Práctica recomendada: Defina planificaciones que procesen los datos del supervisor de uso de almacenamiento intermedio a la hora y 10 minutos y los datos de utilización de unidad a la hora y 40 minutos.
   d. En la pantalla Subir datos pulse opcionalmente Ejecutar una vez ahora para subir inmediatamente los datos.
2. Para un entorno gestionado centralmente o para un sistema autónomo, defina una planificación para procesar los datos de utilización de unidad. En un entorno gestionado centralmente, sólo es necesario definir la planificación de utilización de unidad en el gestor central.
   a. Vaya a Gestionar > Utilización de unidad > Niveles de utilización de unidad.

b. En la pantalla Niveles de utilización de unidad, pulse Modificar planificación para definir una planificación para procesar los datos de utilización de unidad. Pulse Guardar después de definir una planificación y, a continuación, pulse Atrás para volver a la pantalla Niveles de utilización de unidad. Un punto de partida razonable para muchos despliegues es planificar el proceso para que se ejecute una vez cada hora, pero es posible que desee ajustar el intervalo según los recursos disponibles o las necesidades de datos.
Importante: Para asegurarse de que los datos más recientes están disponibles para los informes de utilización de unidad, defina una planificación que procese los datos de utilización de unidad después de procesar los datos del supervisor de uso de almacenamiento intermedio.
Práctica recomendada: Defina planificaciones que procesen los datos del supervisor de uso de almacenamiento intermedio a la hora y 10 minutos y los datos de utilización de unidad a la hora y 40 minutos.
c. En la pantalla Niveles de utilización de unidad, pulse opcionalmente Ejecutar una vez ahora para procesar inmediatamente los datos.

Resultados

Después de completar estos pasos, vaya a Gestionar > Informes > Utilización de unidad para ver los informes de utilización de unidad. En un entorno gestionado centralmente, los datos estarán disponibles para el gestor central y sus unidades gestionadas. Para un sistema autónomo, los datos sólo estarán disponibles para ese sistema individual. Si no ha utilizado la opción Ejecutar una vez ahora al definir las planificaciones, debe esperar hasta que esos procesos se ejecuten antes de que los informes de utilización de unidad se actualicen con los datos más recientes.
Tema principal: Nivel de utilización de unidad

Subidas de cliente

Database Activity Monitor Content Subscription (denominado anteriormente Database Protection Subscription Service) da soporte al mantenimiento de pruebas de asesoramiento predefinidas, pruebas basadas en SQL, CVE, APAR y grupos como por ejemplo versiones y parches de base de datos.

Las subidas se utilizan para mantener la información actualizada y dentro de las mejores prácticas del sector como protección frente a nuevas vulnerabilidades descubiertas. La distribución de las actualizaciones se realiza trimestralmente.

Utilice Subidas de cliente para subir lo siguiente: archivos de actualización DPS; controladores JDBC de Oracle; controladores JDBC de MS SQL Server; y archivos jar de licencia de DB2 para z/OS.

Nota: Si existe un grupo personalizado con el mismo nombre que un grupo de Guardium predefinido, el proceso de subida añadirá Guardium delante del nombre para el grupo predefinido.

1. Abra Subidas de cliente pulsando Reforzar > Asesoramiento de vulnerabilidades > Subidas de cliente.
2. Para Subida de DPS, pulse Examinar para localizar y seleccionar el archivo que se va a subir.
   Nota: Consulte el panel Importar DPS para ver qué archivos se han subido.
3. Para Subir jar de licencias de DB2 z/OS, pulse Examinar para localizar y seleccionar el archivo.
4. Utilice Subir controlador JDBC de Oracle o Subir controlador JDBC de MS SQL Server para subir los controladores de código abierto. Después de subirlo, verá las bases de datos añadidas al Buscador de orígenes de datos. Suba un controlador cada vez.
   Nota: Hay dos instancias en las que se recomiendan controladores de código abierto a través de controladores Data Direct de Oracle o controladores Data Direct de MS SQL.
   a. Para dar soporte a la autenticación de Windows para MS SQL Server. En todos los demás usos, el controlador Data Direct subido previamente en el dispositivo Guardium es suficiente.
   b. Cuando se utiliza la aplicación Seguimiento de cambios de valores para Oracle versión 10 o superior, se recomienda utilizar el controlador de código abierto para dar soporte a la utilización de corrientes de datos en lugar de desencadenantes.

   Utilice palabras clave para buscar y descargar controladores JDBC de código abierto (por ejemplo: *controlador JDBC de código abierto para MS SQL*).

5. Utilice el Gestor central para distribuir el archivo .jar a las unidades gestionadas. Una vez que el archivo se ha subido correctamente, la interfaz gráfica de usuario debe reiniciarse en el Gestor central y en las unidades gestionadas.

Nota:

Si va a exportar e importar definiciones de una unidad a otra, tenga en cuenta que los grupos suscritos no se exportan. Cuando se exportan definiciones que hacen referencia a grupos suscritos, debe asegurarse de que todos los grupos suscritos referenciados están instalados en la unidad de importación (o gestor central en un entorno federado).

Cuando se suban archivos jar de licencia de DB2 z/OS, la licencia se aplicará tras el reinicio de la interfaz gráfica de usuario.

Nota: Si el DPS se detiene por algún motivo (por ejemplo, un reinicio del servidor o un reinicio de la interfaz gráfica de usuario), se recomienda que espere 30 minutos antes de iniciar de nuevo el proceso de subida de DPS.

Habilite ASO en el servidor Oracle utilizando el último controlador DataDirect de Oracle.

Consulte lo siguiente cuando habilite ASO en el servidor Oracle utilizando el último controlador DataDirect de Oracle.

SQLNET.CRYPTO_CHECKSUM_SERVER = required

SQLNET.ENCRYPTION_SERVER = required

SQLNET.ENCRYPTION_TYPES_SERVER = (AES256, AES192, AES128)

#SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER = (SHA256)

SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER = (SHA1)

El controlador JDBC de Oracle funcionará y no requiere que se especifique ninguna propiedad de conexión.

Sin embargo, el último controlador JDBC de Oracle debe descargarse de Oracle. El nombre de archivo es ojdbc7.jar. Utilice palabras clave para buscar y descargar controladores JDBC de código abierto (por ejemplo: controlador JDBC de código abierto para Oracle). A continuación, suba ese controlador en el dispositivo utilizando la función Subidas de cliente de Guardium.

Si continúa utilizando el controlador DataDirect de Oracle, es necesario que especifique una propiedad de conexión para el origen de datos.

Utilice lo siguiente al definir la propiedad de conexión del controlador DataDirect de Oracle:

DataIntegrityLevel=required;EncryptionLevel=required;DataIntegrityTypes=(MD5,SHA1)

Nota: El controlador DataDirect de Oracle actual no da soporte a SHA-256. Por lo tanto, se debe utilizar SHA-1. Es por la razón por la que se tuvo que comentar la referencia de sqlnet.ora (#SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER = (SHA256)). Sin embargo, si un cliente de Guardium debe conectarse utilizando SHA-256, debe utilizar en su lugar el controlador JDBC de Oracle.

Referencias de Data Direct:

https://www.progress.com/documentation/datadirect-connectors

Para obtener una lista de referencias de mandatos, descargue el PDF Guía del usuario de JDBC de base de datos de Oracle.

Utilice un archivo delimitado por tabuladores (.TXT) para crear y guardar un archivo de subida de origen de datos desde la funcionalidad Subidas de cliente

Si opta por utilizar una estructura de archivos delimitados por comas (.CSV), no tendrá el comportamiento esperado si algún valor de columna contiene una coma.

Siga estos pasos

1. Si utiliza EXCEL, guarde el archivo como un archivo delimitado por tabuladores (.TXT).
2. Si utiliza OpenOffice o Libre Office, guarde un archivo (.CSV) con tabulaciones como delimitadores.
3. Inicie sesión como usuario de administración y abra Subidas de cliente pulsando Reforzar > Control de cambios de configuración (Aplicación CAS) > Cargas de cliente.
4. Para Subir CSV para crear/actualizar orígenes de datos, pulse Examinar..., y seleccione el archivo delimitado por tabuladores.

Crear origen de datos para CSV subido mediante el menú Subir CSV

Siga los pasos siguientes para crear un archivo con formato .TXT delimitado por tabuladores que contenga información de origen de datos. A continuación, este archivo .TXT delimitado por tabuladores se puede utilizar con la función Subidas de cliente en la aplicación Subir de Guardium para muchos tipos de orígenes de datos.

La utilización de la función para importar orígenes de datos no ha sido siempre compatible con todos los releases de software de Guardium. Este procedimiento habilitará la subida de cualquier origen de datos.

A continuación se muestra una lista de columnas de cabecera que se deben añadir a una hoja de cálculo Excel cuando se crea el archivo de subida de origen de datos .TXT delimitado por tabuladores:

Valores de columna (aceptados para el archivo de subida de origen de datos .CSV)

Tabla 1. create_datasource

Parámetro	**Descripción**
application	Necesario. Identifica la aplicación para la que se está definiendo el origen de datos. Debe ser una de las opciones siguientes: ChangeAuditSystem Access_policy MonitorValues DatabaseAnalyzer AuditDatabase CustomDomain Classifier AuditTask SecurityAssessment Replay Stap_Verification
compatibilityMode	Modalidad de compatibilidad: Las opciones son Default o MSSQL 2000. Se indica al procesador la modalidad de compatibilidad que se debe utilizar al supervisar una tabla.
conProperty	Opcional. Utilícelo sólo si se deben incluir propiedades de conexión adicionales en el URL de JDBC para establecer una conexión JDBC con este origen de datos. El formato necesario es propiedad=valor, donde cada par de propiedad y valor está separado del siguiente mediante una coma. Para una base de datos Sybase con un conjunto de caracteres predeterminado de Roman8, especifique la propiedad siguiente: charSet = utf8
customURL	Opcional. Serie de conexión con el origen de datos; de lo contrario, la conexión se realiza utilizando el host, puerto, instancia, propiedades, etc. de los campos especificados anteriormente. Como ejemplo, esto resulta útil para crear conexiones de Oracle Internet Directory (OID).
dbInstanceAccount	Opcional. Nombre de inicio de sesión de la cuenta de base de datos (propietario de software) que utilizará CAS
dbInstanceDirectory	Opcional. Directorio donde se ha instalado el software de base de datos que utilizará CAS
dbName	Opcional. Para un origen de datos DB2 u Oracle, especifique el nombre de esquema. Para otros, especifique el nombre de la base de datos.
description	Opcional. Descripción más larga del origen de datos.
host	Necesario. Puede ser el nombre de host o la dirección IP.
name	Necesario. Proporciona un nombre exclusivo para el origen de datos en el sistema.

Parámetro	Descripción
owner	Necesario. Identifica la cuenta de usuario de Guardium que es propietaria del origen de datos.
password	Opcional. Contraseña del propietario. Si se utiliza, el usuario también debe utilizarse.
port	Opcional (entero). Número de puerto.
serviceName	Necesario para Oracle, Informix, DB2 y IBM® ISeries. Para un origen de datos DB2, especifique el nombre de la base de datos; para otros, especifique el nombre del servicio.
severity	Opcional. Clasificación de gravedad (o nivel de impacto) para el origen de datos.
shared	Opcional (booleano). Establézcalo en **true** para compartir con otras aplicaciones. Para compartir el origen de datos con otros usuarios, tendrá que asignar roles desde la interfaz gráfica de usuario.
type	Necesario. Identifica el tipo de origen de datos; debe ser uno de los siguientes: DB2 DB2 for i DB2 for z/OS Informix MS SQL Server MS SQL Server (DataDirect) MySQL N/D Netezza Oracle (DataDirect) Oracle (nombre de servicio) Oracle (SID) PostgreSQL Sybase Sybase IQ Teradata Se puede utilizar lo siguiente cuando la aplicación es CustomDomain o Classifier: TEXT TEXT:FTP TEXT:HTTP TEXT:HTTPS TEXT:SAMBA
user	Opcional. Usuario del origen de datos. Si se utiliza, también se debe utilizar la contraseña.
environmentTitle	Necesario para la protección de servicio de base de datos de nube. Nombre de la cuenta.
region	Necesario para la protección de servicio de base de datos de nube. Región AWS.
objectLimit	Necesario para la protección de servicio de base de datos de nube. El número máximo de objetos encontrados en el proceso de clasificación que se añaden automáticamente a la lista de objetos auditados. Consulte Protección del servicio de base de datos de nube.
primaryCollector	Necesario para la protección de servicio de base de datos en la nube. El recopilador que extrae los datos de auditoría de la base de datos de nube.

Notas:

1. Cada uno de los nombres de columna debe incluirse en la hoja de cálculo de Excel GUARDADA como un archivo delimitado por tabuladores (.TXT).
2. El nombre del origen de datos creado (que se muestra al buscar el origen de datos) se compone del nombre de columna y del tipo de columna.
3. El archivo de subida se DEBE guardar como un tipo de archivo de columnas delimitado por tabuladores.

Pasos para crear y subir un archivo de texto con formato CSV y añadir datos de origen de datos

1. Cree el archivo de hoja de cálculo de Excel como un archivo .TXT delimitado por tabuladores con las siguientes cabeceras y datos de origen de datos para dar soporte a la capacidad de importación del origen de datos.
2. Cree y guarde el archivo .txt en su PC o en el dispositivo de UNIX/Linux para su subida a la aplicación de Guardium.
3. Inicie sesión como usuario de administración y abra Subidas de cliente pulsando Reforzar > Control de cambios de configuración (Aplicación de CAS) > Cargas de cliente

4. En Subir CSV para crear/actualizar orígenes de datos, pulse Examinar y seleccione el archivo .txt delimitado por tabuladores que contiene la información de origen de datos.
5. Pulse Subir.

Aparecerá un mensaje en el que se mostrarán qué valores del archivo .txt se han subido:

1. **Nuevo**: por subida de archivo (si se guarda el archivo y los miembros Nuevo origen de datos añadidos, estos miembros tendrán el estado de NUEVO).
2. **Actualizar**: Subir el MISMO origen de datos en el que haya realizado los cambios le dará estado Actualizar.
3. **Error**: Se visualiza un origen de datos fallido o un error

Tema principal: Gestión del sistema Guardium

Panel Estado de Servicios

El panel Estado de servicios es una ubicación centralizada donde comprobar el estado de los servicios como, por ejemplo, CAS o el alertador, y, si es necesario, investigar con mayor detalle cada servicio. Abra el panel Estado de servicios pulsando Configuración > Herramientas y Vistas > Estado de servicios. Cada vez que se abre el panel Estado de servicios, se renueva el estado de cada servicio.

Supongamos que se configura una política que envía una alerta en tiempo real siempre que hay más de tres inicios de sesión fallidos en 5 minutos. Para protegerse contra esta posible intrusión, debe asegurarse de que la política se ha instalado y de que el alertador está activo.

Utilice el panel Estado de servicios para verificar que estos dos servicios se hayan configurado correctamente.

Si pulsa cualquier servicio, irá a su página de configuración, donde puede, según corresponda, activar o desactivar el servicio, reiniciar un servicio, configurar un servicio, etc.

Si por algún motivo la política no se ha instalado correctamente, pulse Configuración > Herramientas y Vistas > Instalación de políticas para ir a Instalador de políticas, ver las políticas instaladas actualmente y realizar los cambios necesarios.

Cada servicio muestra uno de los iconos siguientes:

- El servicio está en ejecución/planificado:
- El servicio está en pausa:
- El servicio está desactivado:

Tema principal: Gestión del sistema Guardium

Archivado, depuración y restauración

Las operaciones de archivado y depuración se deberían ejecutar de forma planificada. Utilice Archivado de datos y Archivado de resultados para almacenar la información capturada y la información para auditoría. Copia de seguridad y archivado Amazon S3 en Guardium también aparece al final de este tema.

Puede encontrar Archivado de datos y Archivado de resultados pulsando Gestionar > Gestión de datos.

- Archivado de datos hace copia de seguridad de los datos capturados por el sistema Guardium, durante un periodo de tiempo. Cuando se configure el Archivado de datos, también se debe configurar una operación de depuración. Normalmente los datos se archivan diariamente al final del día para garantizar que, en caso de catástrofe, sólo se pierda un día de datos. La depuración de los datos depende de la aplicación y varía considerablemente, según los requisitos empresariales y de auditoría. En la mayoría de los casos, los datos se pueden mantener en los sistemas Guardium durante más de seis meses.
- Archivado de resultados hace copia de seguridad de los resultados de tareas de auditoría (informes, pruebas de asesoramiento, seguimiento de auditoría de entidad, conjuntos de privacidad y procesos de clasificación) así como de los seguimientos de aprobaciones y visualizaciones y los comentarios alojados de los procesos de flujo de trabajo. Los conjuntos de resultados se depuran del sistema según la definición del proceso de flujo de trabajo.

En un entorno de agregación, se pueden archivar datos del recopilador, del agregador o de ambas ubicaciones. Habitualmente los datos se archivan una sola vez, y la ubicación desde la que se archivan varía según sus requisitos.

Las operaciones de exportación planificadas envían datos desde las unidades de recopilador de Guardium a un servidor de agregación de Guardium. En su propia planificación, el servidor de agregación ejecuta una operación de importación para completar el proceso de agregación. En una de estas unidades, o en ambas, se planifican las operaciones de archivado y depuración para hacer copia de seguridad y depurar los datos regularmente (tanto para liberar espacio como para agilizar las operaciones de acceso en la base de datos interna).

Los archivos de archivado se pueden enviar utilizando el protocolo SCP o FTP, o a un sistema de almacenamiento EMC Centera o TSM (si está configurado). Puede definir una única configuración de archivado para cada sistema Guardium.

La función de archivado de Guardium crea archivos firmados y cifrados que no se pueden manipular. NO cambie los nombres de los archivos de archivado generados. Las operaciones de archivado y restauración dependen de los nombres de archivo que se crean durante el proceso de archivado.

Las actividades de archivado y exportación utilizan el secreto compartido del sistema para crear archivos de datos cifrados. Para que se pueda restaurar la información cifrada de un sistema en otro, primero debe tener el secreto compartido utilizado en el sistema de archivado cuando se creó el archivo.

Siempre que archive datos, asegúrese de verificar que la operación se completa correctamente. Para ello, abra el Registro de agregación/archivado pulsando Gestionar > Informes > Gestión de datos > Registro de agregación/archivado. Debería haber varias actividades listadas para cada operación de archivado, y el estado de cada actividad debería ser Completado.

Realice tareas de copia de seguridad del sistema pulsando Gestionar > Gestión de datos > Copia de seguridad del sistema. También puede realizar tareas de copia de seguridad desde la CLI. Consulte Mandatos de CLI de manejo de archivos para obtener información adicional.

Depuración predeterminada

- El valor predeterminado para depuración es 60 días

- La actividad de depuración predeterminada está planificada diariamente a las 5:00 AM.
- Para una nueva instalación, la planificación de depuración predeterminada se instala en función del valor y actividad predeterminados.
- Cuando un tipo de unidad se cambia a unidad gestionada o de nuevo a unidad autónoma, se aplica la planificación de depuración predeterminada.
- Una actualización no afectará de ninguna forma a la planificación de depuración.
- Cuando se depure un gran número de registros (10 millones o más), el método más efectivo es un valor de tamaño de lote grande (de 500 000 a 1 millón). Si se utiliza un tamaño de lote más pequeño o NULL, la depuración tardará muchas más horas. Las depuraciones más pequeñas finalizan rápidamente, por lo que el valor de tamaño de lote grande sólo es relevante para las depuraciones más grandes.

Nota: No se puede establecer el tamaño de lote en la interfaz de usuario. Para establecer el tamaño de lote, utilice el mandato de GuardAPI grdapi set_purge_batch_size batchSize.

Cómo determinar qué días no se archivan

Utilice el Creador de informes para ver la lista de todos los archivos con las fechas de archivado. Abra el Creador de informes pulsando Gestionar > Informes > Creador de informes. En el menú Consulta, seleccione Vista de ubicación. Las fechas que no están en ese informe son las fechas que no se han archivado. Ejecute el archivado para las fechas que no están en la lista, si así se requiere.

Configurar archivado y depuración de datos

1. Abra el Archivado de datos pulsando Gestionar > Gestión de datos > Archivado de datos.
2. Para archivar, marque el recuadro de selección Archivar. Aparecerán campos adicionales en el panel Configuración.
3. Para Archivar datos anteriores a, especifique un valor y seleccione una unidad de tiempo en el menú. Para archivar los datos a partir de los datos de ayer, especifique el valor `1` y seleccione Día(s) en el menú.
4. Utilice Ignorar datos anteriores a para controlar cuántos días de datos se archivarán. Cualquier valor especificado aquí debe ser mayor que el valor Archivar datos anteriores a.
   Nota: Si deja este campo en blanco, archivará datos para todos los días con una antigüedad superior al valor especificado en Archivar datos anteriores a. Esto significa que si archiva diariamente y depura datos anteriores a 30 días, se archiva cada día de datos 30 veces (antes de que se depure el día 31).
5. Marque el recuadro de selección Archivar valores para incluir valores de series SQL en los datos archivados. Si se desmarca este recuadro, los valores se sustituyen por signos de interrogación en el archivado (y por lo tanto los valores no estarán disponibles tras una operación de restauración).
6. Seleccione una opción Protocolos y rellene la información adecuada. En función de cómo se haya configurado el sistema Guardium, es posible que uno de estos botones no esté disponible. Para ver una descripción de cómo configurar los métodos de almacenamiento de archivado y copia de seguridad, consulte la descripción de los mandatos del sistema show storage y store storage.
7. Realice el procedimiento adecuado, según el método de almacenamiento seleccionado:
   - Configurar archivado o copia de seguridad SCP o FTP
   - Configurar archivado o copia de seguridad EMC Centera
   - Configurar archivado o copia de seguridad TSM
8. Marcar el recuadro de selección Depurar para definir una operación de depuración.

   IMPORTANTE: La configuración de depuración la utilizan tanto el archivado de datos como la exportación de datos. Los cambios realizados aquí se aplican a todas las ejecuciones de exportación de datos, y viceversa. En el caso de que la depuración esté activada y que la exportación de datos y el archivado de datos se ejecuten el mismo día, la primera operación que se ejecute probablemente depurará los datos anteriores antes de que se ejecute la segunda operación.

   Por esta razón, cuando están configurados tanto la exportación de datos como el archivado de datos, la antigüedad de depuración debe ser mayor que la antigüedad de la exportación y la antigüedad del archivado.

9. Si se depuran datos, utilice el campo Depurar datos anteriores a para especificar el día de inicio de la operación de depuración como el número de días, semanas y meses anteriores al día actual, que es cero. Todos los datos del día especificado y todos los días anteriores se depuran, excepto según se indique. Cualquier valor especificado para la fecha de inicio de depuración debe ser mayor que el valor especificado para el valor Archivar datos anteriores a. Además, si la exportación de datos está activa, la fecha de inicio de depuración especificada aquí debe ser mayor que el valor Exportar datos anteriores a. Consulte la nota IMPORTANTE.
   Nota:

   No hay ningún aviso cuando se depuran datos que no han sido archivados o exportados por una operación anterior.

   La operación de depuración no depura los datos restaurados cuya antigüedad está dentro del marco de tiempo de No depurar datos restaurados en una operación de restauración.

10. Utilice la sección Planificación para definir una planificación para ejecutar esta operación regularmente.
11. Pulse Guardar para guardar los cambios de configuración. El sistema intenta verificar la configuración enviando un archivo de datos de prueba a esa ubicación.
    - Si la operación falla, se muestra un mensaje de error y la configuración no se guardará.
    - Si la operación se realiza correctamente, la configuración se guarda.
12. Pulse Ejecutar una vez ahora para ejecutar la operación una vez.

Configurar archivado o copia de seguridad SCP o FTP

Después de seleccionar SCP o FTP en un panel de configuración de archivado o copia de seguridad, debe proporcionar la siguiente información:

1. Para Host, especifique la dirección IP o nombre de host del host que recibirá los datos archivados.
2. Para Directorio, identifique el directorio en el que se almacenarán los datos. La manera de especificar esto dependerá de si el método de transferencia de archivos es FTP o SCP.
   - Para FTP: Especifique el directorio relativo al directorio de inicio de la cuenta FTP.
   - Para SCP: Especifique el directorio como una vía de acceso absoluta.
3. Para Puerto: Especifique el puerto que se puede utilizar para enviar archivos a través de SCP y FTP. El puerto predeterminado para ssh/scp/sftp es 22. El puerto predeterminado para FTP es 21.
   Nota: Si ve un cero (0) como puerto, esto indica que se utiliza el puerto predeterminado y que no es necesario cambiarlo.
4. Para Nombre de usuario y Contraseña, especifique las credenciales del usuario que inicia sesión en el servidor SCP o FTP. Este usuario debe tener permisos de escritura/ejecución para el directorio especificado en Directorio.

   Para Windows, se acepta un usuario de dominio con el formato de dominio\usuario

5. Pulse Guardar para guardar la configuración.

Configurar archivado o copia de seguridad EMC Centera

Esta tarea de copia de seguridad o archivado copia archivos en el sistema de almacenamiento remoto EMC Centera. Se requiere una licencia con nombre de usuario y contraseña de EMC. Se requieren cuatro acciones principales para esta tarea:

1. Establecer cuenta con un EMC Centera en la red (se requieren direcciones IP y un ClipID)
2. Configurar los datos y/o archivos de configuración de un sistema Guardium
3. Definir y exportar una biblioteca
4. Confirmar que sus archivos se almacenan en el sistema de almacenamiento EMC Cetera.

Acción de la CLI

Desde la CLI, ejecute estos mandatos:

```
store storage-system centera backup ON
show storage-system
```

Configurar archivado o copia de seguridad Centera

Abra Copia de seguridad del sistema pulsando Gestionar > Gestión de datos > Copia de seguridad del sistema. Seleccione EMC Centera. Debe proporcionar la siguiente información:

1. Para Retención, especifique el número de días que se retendrán los datos. El máximo es 24855 (68 años). Si desea guardarlos más tiempo, puede restaurar los datos posteriormente y volver a guardarlos.
2. Para Dirección de agrupación de Centera, especifique la serie de agrupación de conexión de Centera; por ejemplo:
   10.2.3.4,10.6.7.8?/var/centera/us1_profile1_rwe.pea txt
   Nota: Esta dirección IP y el archivo .PEA proceden de EMC Centera. Cuando se configura la vía de acceso, se requiere el signo de interrogación. El nombre de vía de acceso .../var/centera/... es importante, ya que la copia de seguridad podría fallar si no se sigue el nombre de vía de acceso. El archivo .PEA proporciona permisos, nombre de usuario y autenticación de contraseña para cada solicitud de copia de seguridad de Centera.
3. Pulse Subir archivo PEA para subir un archivo PEA de Centera que se utilizará para la serie de conexión. Aún se necesita la dirección de agrupación de Centera.
   Nota: Si aparece el mensaje `No se puede abrir la agrupación en esta dirección...`, compruebe el tamaño del nombre de host del sistema Guardium. Se ha informado de un problema de tiempo de espera con Centera cuando se utilizan nombres de host con una longitud inferior a 4 caracteres.
4. Pulse Guardar para guardar la configuración. El sistema intenta verificar la dirección de Centera abriendo una agrupación utilizando la serie de conexión especificada. Si la operación falla, se le informará y la configuración no se guardará.
5. Pulse Ejecutar una vez ahora para realizar la copia de seguridad utilizando el archivo .PEA descargado.

Confirme que los archivos se han copiado en EMC Centera. Se requiere el nombre de los archivos y un ClipID para esta tarea.

Configurar archivado o copia de seguridad TSM

Antes de archivar en un servidor TSM, se debe subir un archivo de configuración dsm.sys al sistema Guardium, mediante la CLI. Utilice el mandato de CLI import tsm config. Después de seleccionar TSM en un panel de configuración de archivado o copia de seguridad, proporcione la siguiente información:

1. Para Contraseña, especifique la contraseña de TSM que utiliza este sistema Guardium para solicitar los servicios de TSM, y vuelva a especificarla en el recuadro Vuelva a especificar la contraseña.
2. Opcionalmente, especifique un nombre de servidor que coincida con una entrada servername del archivo dsm.sys.
3. Opcionalmente, especifique un nombre Como host.
4. Pulse Guardar para guardar la configuración. Al pulsar el botón Guardar, el sistema intenta verificar el destino de TSM enviando un archivo de prueba al servidor mediante el mandato dsmc archive. Si la operación falla, se le informará y la configuración no se guardará.
5. Vuelva al procedimiento de archivado o copia de seguridad para completar la configuración.

Configurar archivado de resultados

1. Abra el Archivado de resultados pulsando Gestionar > Gestión de datos > Archivador de resultados (auditoría).
2. En los recuadros a continuación de Archivar resultados anteriores a, especifique un día de inicio para la operación de archivado como un número de días, semanas o meses anteriores al día actual, que es el día cero. Para archivar resultados a partir de los datos de ayer, especifique el valor 1, y seleccione Día(s) en la lista.
3. Opcionalmente, utilice los campos a continuación de Ignorar resultados anteriores a para controlar cuántos días de resultados se archivarán. Cualquier valor especificado aquí debe ser mayor que el valor de Archivar resultados anteriores a.
4. Seleccione un método de almacenamiento en los botones de selección. En función de cómo se haya configurado el sistema Guardium, puede haber disponible uno o varios de estos botones. Para ver una descripción de cómo configurar los métodos de almacenamiento de archivado y copia de seguridad, consulte la descripción para mostrar los mandatos show storage-system y store storage-system en Mandatos de CLI de configuración y control.
   - EMC CENTERA
   - TSM
   - SCP
   - FTP
5. Realice el procedimiento adecuado en función del método de almacenamiento seleccionado:
   - Configurar archivado o copia de seguridad SCP o FTP
   - Configurar archivado o copia de seguridad EMC Centera
   - Configurar archivado o copia de seguridad TSM
   - Copia de seguridad y archivado Amazon S3 en Guardium
6. Utilice la sección Planificación para definir una planificación para ejecutar esta operación regularmente.
7. Pulse Guardar para verificar y guardar los cambios de configuración. El sistema intenta verificar la configuración enviando un archivo de datos de prueba a esa ubicación.
   - Si la operación falla, se muestra un mensaje de error y la configuración no se guardará.
   - Si la operación se realiza correctamente, la configuración se guarda.
8. Pulse Ejecutar una vez ahora para ejecutar la operación una vez.

Restaurar datos

Si este sistema no es el sistema que ha generado el archivado que se restaurará, debe crear una entrada de ubicación en el catálogo mediante Archivador de catálogo y, a continuación, pulsar Añadir (consulte: catálogo de Guardium) o GuardAPI (consulte: CLI y API > Referencia de GuardAPI > Funciones de entrada de catálogo de GuardAPI). Cuando se inicie la restauración de datos, esta información se utilizará para transferir el archivo al sistema antes de procesar los datos.

Antes de restaurar los datos

- Antes de restaurar desde TSM, se debe subir un archivo de configuración dsm.sys al sistema Guardium, mediante la CLI. Utilice el mandato de CLI import tsm config.
- Antes de restaurar desde EMC Centera, se debe subir un archivo PEA al sistema Guardium, mediante el panel Archivado de datos.
- Antes de restaurar o importar un archivo cifrado por otro sistema Guardium, asegúrese de que el secreto compartido del sistema utilizado por el sistema Guardium está disponible en este sistema (de lo contrario, no podrá descifrar el archivo). Consulte Acerca del secreto compartido del sistema en Configuración del sistema.
- Antes de restaurar en un recopilador de Guardium, ejecute el mandato de CLI stop inspection-core para detener el proceso inspection-core.
  Nota: No se pueden capturar los datos durante el proceso de restauración.

Para restaurar los datos:

1. Abra Restaurar datos pulsando Gestionar > Gestión de datos > Restauración de datos.
2. Especifique una fecha en Desde para especificar la fecha más temprana para la que desea datos.
3. Especifique una fecha en Hasta para especificar la fecha más tardía para la que desea datos.
4. Para Nombre de host, especifique opcionalmente el nombre del sistema Guardium desde el que se ha originado el archivado.
5. Pulse Buscar.
6. En el panel Resultados de búsqueda, marque el recuadro de selección Seleccionar para cada archivado que desee restaurar.
7. En el campo No depurar datos restaurados durante al menos, especifique el número de días que desea retener los datos restaurados en el sistema.
8. Pulse Restaurar.
9. Pulse Hecho cuando haya finalizado.

Nota: La restauración de datos archivados desde un recopilador se debe realizar sólo en: el mismo recopilador; un agregador; o un recopilador distinto dedicado a la investigación que no forme parte de un clúster de agregación. En caso de que se cuelgue un recopilador, se debe restaurar una copia de seguridad del sistema en un recopilador completamente nuevo.

Copia de seguridad y archivado Amazon S3 en Guardium

Utilice esta característica para archivar y realizar una copia de seguridad de los datos de Guardium en Amazon S3.

Amazon S3 (Amazon Simple Storage Service) proporciona una interfaz de servicio web sencilla que se puede utilizar para almacenar y recuperar cualquier cantidad de datos, en cualquier momento, desde cualquier lugar de la web. Proporciona a cualquier desarrollador acceso a la misma infraestructura altamente escalable, fiable, segura y económica que utiliza Amazon para ejecutar sus propios sitios web.

Requisitos previos

1. Una cuenta de Amazon.
2. Registro en el servicio S3
3. Se requieren credenciales de Amazon S3 para acceder a Amazon S3. Estas credenciales son:
   - ID de clave de acceso: Identifica al usuario como parte responsable de las solicitudes de servicio. Se debe incluir en cada solicitud. No es confidencial y no es necesario que esté cifrado. (secuencia alfanumérica de 20 caracteres).
   - Clave de acceso secreta: La clave de acceso secreta se asocia al ID de clave de acceso calculando una firma digital incluida en la solicitud. La clave de acceso secreta es un secreto, y sólo el usuario y AWS deberían tenerla (secuencia de 40 caracteres). Esta clave es sólo una larga serie de caracteres (y no un archivo) que se utiliza para calcular la firma digital que se debe incluir en la solicitud.

- El archivado de datos hace copia de seguridad de los datos capturados por el sistema durante un periodo determinado.
- El archivado de resultados hace copia de seguridad de los resultados de tareas de auditoría (informes, pruebas de asesoramiento, seguimiento de auditoría de entidades, conjuntos de privacidad y procesos de clasificación) así como de los seguimientos de aprobaciones y visualizaciones y los comentarios alojados de los procesos de flujo de trabajo.

Cuando se archivan los datos de Guardium, hay un archivo individual para cada día de datos.

Formato de nombre de archivo de datos de archivado:

```
<time>-<nombre_host.dominio>-w<indicación_fecha_y_hora_ejecución>-d<fecha_datos>.dbdump.enc
```

La función de archivado de Guardium crea archivos firmados y cifrados que no se pueden manipular. Los nombres de los archivos de archivado generados no se deben cambiar. La operación de archivado depende de los nombres de archivo creados durante el proceso de archivado.

Las copias de seguridad del sistema se utilizan para realizar copias de seguridad de todos los datos y valores de configuración necesarios y utilizarlos para restaurar un servidor en caso de que el hardware resulte dañado.

Toda la información y los datos de configuración se graban en un único archivo cifrado y se envían al destino especificado, utilizando el método de transferencia configurado para las copias de seguridad en este sistema.

Formato de archivo de sistema de copia de seguridad:

```
<fecha_datos>-<hora>-<nombre_host.dominio>-SQLGUARD_CONFIG-9.0.tgz
<fecha_datos>-<time>-<nombre_host.dominio>-SQLGUARD_DATA-9.0.tgz
```

Utilice el informe Registro de agregación/archivado en Guardium para verificar que la operación se completa correctamente. Abra el Registro de agregación/archivado pulsando Gestionar > Informes > Gestión de datos > Registro de agregación/archivado. Debe haber varias actividades listadas para cada operación de archivado, y el estado de cada actividad debería ser *Satisfactorio*.

Independientemente del destino de los datos archivados, el catálogo de Guardium realiza un seguimiento de dónde se envía cada archivo de archivado, para que se pueda recuperar y restaurar en el sistema con el mínimo esfuerzo en cualquier momento en el futuro.

Se mantiene un catálogo individual en cada sistema, y se añade un nuevo registro al catálogo cada vez que el sistema archiva datos o resultados.

Las entradas de catálogo se pueden transferir entre dispositivos mediante uno de los métodos siguientes:

- Agregación: Se agregan tablas de catálogo, lo que significa que el agregador tendrá el catálogo fusionado de todos sus recopiladores

- Exportar/Importar catálogo: Estas funciones se pueden utilizar para transferir entradas de catálogo entre recopiladores, o para hacer copia de seguridad de un catálogo para su restauración posterior, etc.
- Restauración de datos: Cada operación de restauración de datos contiene los datos del día archivado, incluido el catálogo de ese día. Por lo tanto, al restaurar datos, el catálogo también se actualiza.

Cuando se importen entradas de catálogo de otro sistema, estas entradas apuntarán a archivos que ese sistema ha cifrado. Antes de restaurar o importar un archivo de este tipo, el secreto compartido del sistema correspondiente al sistema que ha cifrado el archivo debe estar disponible en el sistema de importación.

Habilite Amazon S3 desde la CLI de Guardium

La opción de copia de seguridad y archivado Amazon S3 no está habilitada de forma predeterminada en la interfaz gráfica de usuario de Guardium. Para habilitar Amazon S3 mediante la CLI de Guardium, ejecute los siguientes mandatos de CLI:

```
store storage-system amazon_s3 archive on
store storage-system amazon_s3 backup on
```

Amazon S3 requiere que la hora del reloj del sistema Guardium sea correcta (menos de 15 minutos de desviación). De lo contrario, esto producirá un error de Amazon. Si hay una diferencia demasiado grande entre la hora de la solicitud y la hora actual, la solicitud no se aceptará.

Si la hora del sistema Guardium no es correcta, establezca la hora correcta mediante los siguientes mandatos de CLI:

```
show system ntp server
store system ntp server (Un ejemplo es ntp server: ntp.swg.usma.ibm.com)
store system ntp state on
```

Interfaz de usuario

Utilice la Copia de seguridad del sistema para configurar la copia de seguridad. Abra la Copia de seguridad del sistema pulsando Gestionar > Gestión de datos > Copia de seguridad del sistema.

La entrada de usuario requiere:

- Nombre de bucket S3 (cada objeto almacenado en Amazon S3 está contenido en un bucket. Los buckets particionan el espacio de nombres de los objetos almacenados en Amazon S3. En un bucket, puede utilizar cualquier nombre para sus objetos, pero los nombres de bucket deben ser exclusivos en todo Amazon S3.
- ID de clave de acceso
- Clave de acceso secreta

Si el nombre de bucket no existe, se creará.

La clave de acceso secreta se cifra cuando se guarda en la base de datos.

Compruebe que los archivos no se han subido en Amazon S3

1. Inicie sesión en AWS Management Console utilizando su dirección de correo electrónico y contraseña.

http://aws.amazon.com/console/

1. Pulse S3.
2. Pulse el bucket que ha especificado en la interfaz de usuario de Guardium.

Cómo depurar datos del dispositivo de Guardium

Hay dos áreas de un dispositivo de Guardium que pueden llenarse y causar que la interfaz gráfica de usuario se detenga:

- La base de datos interna
- El propio sistema de archivos (normalmente la partición /var)

Como usuario CLI, compruebe si la base de datos está llena con este mandato de CLI:

support show db-status free %

Si se devuelve un 10 % o menos, la base de datos está llena en un 90 % o más.

Para comprobar si la partición /var (sistema de archivos) está llena en un 90 % o más, ejecute un mandato must gather desde la CLI:

support must_gather system_db_info

Debería poder utilizar el servidor de archivos para comprobar si la salida df -k en el archivo system_output.txt se puede ver en el servidor de archivos

must_gather/system_logs/system_output.txt

o si se ha extraído del archivo system.<fecha_hora>.tgz una vez que la ha descargado

En el archivo system_output.txt puede encontrar los detalles.

Here the /var partition is 65% full.

==========2016-11-30 08:36:09 ... Output of df command:==========

Filesystem 1024-blocks Used Available Capacity Mounted on

/dev/sda3 10154020 2272668 7357232 24% /

/dev/sda2 28571320 17384504 9712052 65% /var

/dev/sda1 505604 33476 446024 7% /boot

tmpfs 6169768 0 6169768 0% /dev/shm

Las últimas versiones de Guardium tienen una característica/dispositivo de seguridad que impedirá que los procesos principales recopilen más datos cuando la base de datos o el sistema de archivos alcance un nivel determinado.

El valor predeterminado es detener los procesos cuando la base de datos y/o el sistema de archivos alcanza un nivel de llenado del 90 %, según la documentación de la versión 10.1 de este ejemplo. Puede comprobar el valor actual del dispositivo de seguridad mediante la CLI:

CLI> show auto_stop_services_when_full

Nota: Si auto_stop_services_when_full está desactivado, el dispositivo puede seguir llenando el sistema hasta que esté al 100 %, lo que le impedirá completamente el acceso al sistema.

Nunca debería necesitar o desear establecer auto_stop_services_when_full en OFF, a menos que se trate de un uso temporal en las circunstancias específicas descritas en la respuesta anterior cuando debería utilizarlo tal como se ha descrito antes de activarlo de nuevo una vez que se haya resuelto el problema de espacio.

Nota: Debe detener inspection-core antes de desactivar auto_stop. Esto evitará que el sistema se llene más.

Por lo tanto, en este caso, el sistema detendrá automáticamente inspection-core y otros procesos cuando el sistema de archivos o la base de datos esté llena en el 90 %. Esto incluye la interfaz gráfica de usuario, por lo que no podrá conectarse a la GUI en este momento.

Si intenta reiniciar los servicios detenidos con este mandato, el sistema (y la interfaz de usuario) probablemente se detendrá tras 5 minutos, por la misma razón. restart stopped_services

Nota: Este mandato sólo se debe utilizar una vez si está seguro de que se ha recuperado espacio.

Antes de que la base de datos o el sistema de archivos se llene hasta el nivel "auto stop", debería recibir avisos en el registro del sistema (archivo de mensajes)

Se pueden crear alertas para que reciba un correo electrónico sobre los problemas de espacio antes de que se desencadene auto stop. Consulte Alerta de base de datos llena de Guardium

Puede ejecutar un mandato must_gather y comprobar el archivo comprimido que se crea para ver el último archivo de mensajes que contiene

support must_gather system_db_info

>>>Depuración de datos de la base de datos interna cuando la interfaz gráfica de usuario está inactiva

Si se ha desencadenado auto stop, esto detiene servicios como la interfaz gráfica de usuario, lo que le impide realizar una depuración de emergencia de los datos mediante la opción de depuración "Depurar una vez ahora".

Para realizar una depuración de emergencia, haga lo siguiente:

- Asegúrese de que inspection-core esté desactivado en Recopiladores para impedir que fluyan más datos al dispositivo

stop inspection-core

- Compruebe que no haya NINGÚN mandato de base de datos en ejecución, excepto show processlist (si es necesario, permita que finalicen los mandatos en ejecución antes realizar del paso siguiente)

support show db-processlist running

Debería poder reiniciar simplemente la interfaz gráfica de usuario para acceder a ella para realizar la depuración conforme a ¿Qué puedo hacer si veo que mi dispositivo de Guardium se está llenando?

Si hay un problema por el cual la interfaz gráfica de usuario continúa desactivándose cada 5 minutos, puede considerar desactivar TEMPORALMENTE auto_stop_services_when_full para poder reiniciar la interfaz gráfica de usuario y depurar algunos datos. Si sólo se reinicia la interfaz gráfica de usuario, esta puede mantenerse en ejecución apenas 5 minutos. El proceso nanny principal podría volver a detener los servicios antes de que se depuraran datos suficientes o antes de que hubiera tiempo de poner en marcha la depuración.

Nota: Si auto_stop_services_when_full está desactivado, el dispositivo puede seguir llenando el sistema hasta que esté al 100 %, lo que le impedirá completamente el acceso al sistema.

Nunca debería necesitar o desear establecer auto_stop_services_when_full en OFF, a menos que se trate de un uso temporal en las circunstancias específicas descritas aquí, cuando debería utilizarlo tal como se ha descrito antes de activarlo de nuevo una vez que se haya resuelto el problema de espacio.

Debe detener inspection-core antes de desactivar auto_stop. Esto evitará que el sistema se llene aún más.

CLI> store auto_stop_services_when_full off

CLI> show auto_stop_services_when_full [off | restart | gui]

Ahora puede ir a la interfaz gráfica de usuario y a continuación a Archivado de gestión de datos y poner en marcha una depuración para borrar algunos datos.

Continúe comprobando hasta qué punto está llena la base de datos y el registro de archivado de agregación le mostrará cuándo finalice el proceso de depuración.

Una vez que haya finalizado y tenga espacio en el sistema, debe volver a activar auto_stop y a continuación reiniciar los servicios detenidos de esta forma

store auto_stop_services_when_full on

restart stopped services

Si es necesario, reinicie el núcleo de inspección.

Ahora los datos deberían empezar a recopilarse de nuevo.

Si el sistema se ha llenado, normalmente significa que se está registrando demasiada actividad.

Tema principal: Gestión del sistema Guardium
Información relacionada:
Configuración y gestión avanzadas del sistema Guardium (vídeo)
Cómo evitar problemas de base de datos llena de Guardium y cómo reaccionar a ellos (vídeo)

Catálogo de Guardium

Cuando archiva datos del sistema Guardium, el catálogo de Guardium realiza un seguimiento de dónde se envía cada archivo de archivado, para que se pueda recuperar y restaurar.

Acerca de esta tarea

Se mantiene un catálogo individual en cada sistema Guardium, y se añade un nuevo registro al catálogo cada vez que el sistema archiva datos o resultados. Las entradas de catálogo se pueden transferir entre dispositivos mediante uno de los métodos siguientes:

- Agregación: Se agregan tablas de catálogo, lo que significa que el agregador tiene el catálogo fusionado de todos sus recopiladores.
- Exportar/Importar catálogo: Estas funciones se pueden utilizar para transferir entradas de catálogo entre recopiladores, o para realizar una copia de seguridad de un catálogo para una restauración posterior.
- Restauración de datos: cada operación de restauración de datos contiene los datos del día de archivado, incluido el catálogo de ese día. Cuando se restauran datos, el catálogo también se actualiza.

Puede archivar un catálogo, exportar un catálogo al almacenamiento externo o importar un catálogo que se ha almacenado.

Cuando las entradas de catálogo se importan desde otro sistema, esas entradas apuntan a los archivos que ese sistema ha cifrado. Antes de restaurar o importar cualquier archivo de este tipo, el secreto compartido del sistema que cifró el archivo debe estar disponible en el sistema de importación. Puede utilizar los mandatos de CLI aggregator backup file file y aggregator restore keys file para copiar los secretos compartidos de un sistema Guardium a otro.

Tema principal: Gestión del sistema Guardium

Archivado de un catálogo

Procedimiento

1. Pulse Gestionar > Gestión de datos > Archivador de catálogo.
2. Puede visualizar las entradas de catálogo disponibles para un rango de fechas o añadir una entrada de catálogo. Para visualizar las entradas de catálogo:
   a. Especifique una fecha en Desde para especificar la fecha más temprana para la que desea datos.
   b. Especifique una fecha en Hasta para especificar la fecha más tardía para la que desea datos.
   c. Opcional: Para Nombre de host, especifique el nombre del sistema Guardium desde el que se ha originado el archivado.
   d. Pulse Buscar.

   Para añadir una entrada de catálogo:
   a. Pulse Añadir.
   b. Especifique un Nombre de archivo.
   c. Especifique un Nombre de host.
   d. Especifique la Vía de acceso del archivo.
   Nota:

   Para FTP: Especifique el directorio relativo al directorio de inicio de la cuenta de FTP

   Para SCP: Especifique el directorio como una vía de acceso absoluta.

   Para TSM: Especifique el directorio como una vía de acceso absoluta de la ubicación original.

   e. Especifique un Nombre de usuario y una Contraseña para acceder a esta ubicación.
   f. En el campo Retención, especifique el número de días que esta entrada se va a conservar en el catálogo (el valor predeterminado es 365).
   g. Seleccione una opción en el menú Sistema de almacenamiento en el que está contenido el archivo.
   h. Pulse Guardar.
3. Para eliminar una entrada de catálogo, abra el catálogo, seleccione la entrada y pulse Eliminar seleccionados.
4. Pulse Hecho cuando haya finalizado.

Exportación de un catálogo

Procedimiento

1. Pulse Gestionar > Gestión de datos > Exportación de catálogo.
2. Seleccione un tipo de definición en la lista desplegable Tipo. La lista Definiciones para exportar se llena con definiciones del tipo seleccionado.
3. Seleccione todas las definiciones de este tipo que desea exportar y pulse Exportar. En función de los valores de seguridad del navegador, es posible que vea un mensaje que le solicite si desea guardar el archivo o abrirlo.
4. Elija una ubicación para guardar el archivo exportado.

Importación de un catálogo

Procedimiento

1. Pulse Gestionar > Gestión de datos > Importar catálogo.
2. Pulse Examinar para localizar y seleccionar el archivo.
3. Pulse Subir. Se le notificará cuando se complete la operación y se visualicen las definiciones que están contenidas en el archivo. Repita para subir más archivos.
4. Pulse Importar para importar los archivos subidos o pulse Eliminar sin importar para eliminar los archivos subidos sin importar el contenido.

Cómo gestionar la copia de seguridad y el archivado

Establezca prácticas de retención de datos; controle el volumen de actividad; gestione la planificación del archivado y la depuración de datos y haga copias de seguridad mensuales.

Valor añadido: Mejores prácticas. Protéjase contra la pérdida de datos. Haga que sus datos estén rápidamente accesibles para fines de auditoría.

Utilice la función Copia de seguridad del sistema para definir una operación de copia de seguridad que se pueda ejecutar a petición o de una forma planificada.

Las copias de seguridad del sistema se utilizan para hacer copia de seguridad y almacenar todos los datos y valores de configuración necesarios para restaurar un servidor en caso de que se dañe el hardware.

Hay dos operaciones de archivado disponibles. Vaya a Gestionar > Gestión de datos para seleccionar las funciones Archivado de datos o Archivado de resultados:

- *Archivado de datos* hace copia de seguridad de los datos que ha capturado el sistema Guardium durante un periodo de tiempo determinado. Cuando se configure el Archivado de datos, también se debe configurar una operación de depuración. Normalmente, los datos se archivan al final del día en el que se capturan, lo que garantiza que, en caso de catástrofe, sólo se pierdan los datos de ese día. La depuración de los datos depende de la aplicación y varía considerablemente, según los requisitos empresariales y de auditoría. En la mayoría de los casos, los datos se pueden mantener en las máquinas durante más de seis meses.
- *Archivado de resultados* hace copia de seguridad de los resultados de las tareas de auditoría (informes, pruebas de asesoramiento, seguimiento de auditoría de entidad, conjuntos de privacidad y procesos de clasificación) así como de los seguimientos de aprobaciones y visualizaciones y los comentarios alojados de los procesos de flujo de trabajo. Los conjuntos de resultados se depuran del sistema según la definición del proceso de flujo de trabajo.

En un entorno de agregación, se pueden archivar datos del recopilador, del agregador o de ambas ubicaciones. Habitualmente los datos se archivan una sola vez, y la ubicación desde la que se archivan varía según los requisitos del cliente.

Siempre que archive datos, asegúrese de verificar que la operación se completa correctamente. Para ello, inicie sesión como usuario de administración, y abra Registro de agregación/archivado pulsando Gestionar > Informes > Gestión de datos > Registro de agregación/archivado. Debería haber varias actividades listas para cada operación de archivado, y el estado de cada actividad debería ser *Satisfactorio*.

Copia de seguridad de datos

Hay tres tipos de copias de seguridad de datos recomendadas:

1. Copias de seguridad completas/del sistema:
    a. Copias de seguridad completas semanales o diarias de la unidad de Gestor central (suponiendo que haya un Gestor central autónomo).
    b. Mensual para agregadores y recopiladores durante un periodo tranquilo fuera de horas
2. Archivados diarios (considere estos archivados como copias de seguridad incrementales) para agregadores y recopiladores. Los archivos de archivado de los agregadores son mucho más grandes que los de los recopiladores. Por ejemplo, si un agregador tiene diez recopiladores que le envían datos, el punto de partida del tamaño del archivo de archivador es igual a los de los diez archivos de archivado de los recopiladores. No obstante, es mucho mayor que todos los archivados de recopiladores combinados porque los archivos de archivado de agregador contienen datos adicionales que no envían los recopiladores cada día.
3. Archivado de resultados (es un conjunto especializado de los datos en las copias de seguridad diaria y completa) para agregadores. Una alternativa a la utilización del archivado de resultados es guardar un archivo PDF del proceso de auditoría después de que todos los usuarios hayan completado el proceso de revisión.

Retención de datos

Los archivos de copia de seguridad y archivado tienen dos finalidades: recuperación tras desastre e investigación o auditoría histórica.

Se pueden modificar las sugerencias siguientes en función de la política de retención de datos corporativa. Por ejemplo, algunas organizaciones están obligadas a mantener todas las copias de seguridad durante 18 meses.

Para la recuperación tras desastre

- Mantenga una copia de seguridad completa de tres meses de cada unidad
- Mantenga los archivados diarios de dos semanas continuas de los recopiladores gestionados

Nota: Si tiene recopiladores autónomos, los archivos diarios se deben mantener según su política de retención de datos.

Para fines de auditoría o investigación histórica

- Todos los archivados diarios de los agregadores para el periodo que requieren sus políticas de retención de datos corporativas o su auditoría.

Capacidad de almacenamiento

A continuación se proporcionan sólo estimaciones/rangos de tamaños de archivos de archivado y copia de seguridad para fines de planificación de capacidad de almacenamiento.

Los tamaños reales variarán según (1) el volumen y la granularidad de la actividad de base de datos que se registra en los recopiladores de Guardium, y (2) el periodo de retención de los archivos de copia de seguridad.

Archivados diarios

Recopilador: Aproximadamente de 40 MB (supervisión de usuario privilegiado) a 1 GB (supervisión completa con el registro de todos los detalles sobre todo el tráfico).

Agregador: Un múltiplo aproximado del número de recopiladores, por ejemplo, el número de recopiladores multiplicado por 40 MB.

Copias de seguridad del sistema mensuales – Suponiendo una base de datos llena al 50 % en un Dell R610 o IBM xSeries 3550 M4 (discos de 600 GB)

Nota: La copia de seguridad consigue aproximadamente una compresión 1:8 para el archivo de copia de seguridad.

Recopilador: 7 – 10 GB

Agregador: 16 – 20 GB

Gestor central (sin agregación): << 1 GB

Archivados de resultados

Depende del número y de la frecuencia de los procesos de auditoría implementados.

Controlar el volumen de actividad

El control del volumen de actividad supervisada (en el servidor de base de datos) y registrada (en el recopilador) ayuda a reducir la utilización de red y a reducir el consumo de disco de base de datos del sistema Guardium, y mejora la capacidad y el rendimiento globales de la infraestructura de IBM Security Guardium.

Este control se consigue principalmente en las reglas de política, y mediante la configuración del motor de inspección.

Las directrices generales son las siguientes:

- Evite utilizar rangos de puertos en motores de inspección
- Identifique todas las aplicaciones de confianza y todos los programas por lotes (estos programas normalmente generan la mayor parte de la actividad de base de datos) y, si es posible, ignore/omita su actividad mediante las acciones Ignorar sesión de STAP u Omitir registro.
- A menos que sea necesario, evite utilizar la acción Registrar todos los detalles.
- Si es posible, utilice la política Auditoría selectiva (con las reglas Ignorar sesión de S-TAP) para minimizar el tráfico de red.
- Si no se utilizan reglas de extrusión, por ejemplo, los conjuntos de resultados no se examinan, considere utilizar la acción Ignorar respuestas por sesión para eliminar los conjuntos de resultados que se están enviando al sistema Guardium.
- Establezca un proceso para revisar y actualizar periódicamente las reglas de política, incluidos los grupos, para acomodar las nuevas bases de datos y aplicaciones.
- Establezca un proceso para supervisar periódicamente los errores de SQL y proporcionar a los equipos de desarrollo de aplicaciones y DBA remediación.

Planificación

Las tablas siguientes proporcionan un resumen de las planificaciones clave que se configurarán en los sistemas Guardium. A continuación de las tablas encontrará una breve explicación de cada proceso.

Utilice el Registro de agregación/archivado para registrar la hora y el estado de estos procesos para ayudarle a ajustar sus horas de planificación.

La tabla siguiente lista una planificación de tareas para un sistema Guardium desplegado como recopilador.

Función	**Planificar**
Exportación de datos (a los agregadores)	Diariamente*: 12:30 AM
Archivado y depuración de datos	Diariamente: 01:30 AM Y Depurar durante 15 días
Trabajos de auditoría/Flujo de trabajo	Diariamente: 03:00 AM (si es autónomo)
Exportación de CSV/CEF al servidor SCP/FTP	Diariamente: 05:00 AM, si está configurado en los trabajos de auditoría Y después de que se completen los trabajos de auditoría.
Creación de alias de nombre de host	Diariamente: 10:00 PM
Reinstalación de políticas	Diariamente: 11:00 PM
Copias de seguridad del sistema	Mensualmente: Primer domingo de cada mes a las 6:00 AM

La tabla siguiente lista una planificación de tareas para un sistema Guardium desplegado como agregador.

Función	**Planificar**
Archivado y depuración de datos	Diariamente: 4:00 AM Y Depurar durante 30 días
Importación de datos (de los recopiladores)	Diariamente: 1:15 AM
Trabajos de auditoría/Flujo de trabajo	Diariamente: 03:30 AM
Exportación de CSV/CEF al servidor SCP/FTP	Diariamente: 05:15 AM, si está configurado en los trabajos de auditoría Y después de que se completen los trabajos de auditoría.
Creación de alias de nombre de host	Diariamente: 10:00 PM
Copias de seguridad del sistema	Mensualmente: Primer domingo de cada mes a las 7:00 AM

Nota: Evite planificar antes de las 12:15 a.m. para evitar conflictos con el proceso interno de inicio del día de cada sistema Guardium.

El archivo de datos diario se debe establecer en Archivar datos anteriores a 1 día e Ignorar datos anteriores a 2 días. La primera ejecución archiva todos los datos de la base de datos y los procesos subsiguientes sólo archivarán los datos del día anterior.

La cantidad de datos que se mantiene en línea está limitada por el tamaño de la base de datos en cada sistema Guardium, por lo que el proceso de depuración ayuda a gestionar la cantidad de datos que se mantienen en línea, y funciona con el archivado diario. Guardium recomienda conservar la cantidad mínima de datos necesarios para evitar el llenado de la base de datos y ayudar con el rendimiento de la base de datos.

Para los recopiladores, Guardium recomienda 15 días para el recopilador y 30 días para el agregador. Sin embargo, la duración real depende de la cantidad de datos que se registran (por ejemplo, números de S-TAPS, reglas de política y recopiladores).

Importación e importación de datos

Las actividades registradas del día anterior se exportan diariamente (un proceso de envío) desde los recopiladores a sus agregadores asignados para los informes agregados. Esta actividad es el equivalente a la importación de datos en el agregador.

Nota: Para mayor comodidad, la depuración se puede configurar en las pantallas de configuración Archivar o Exportar.

El proceso de importación de datos sólo se planifica en un agregador. Importa y procesa los datos del día anterior exportados de los recopiladores.

Copias de seguridad mensuales

Como se ha indicado anteriormente, las copias de seguridad del sistema son copias de seguridad completas y se utilizan para la recuperación tras desastre. A continuación se muestra un ejemplo de la planificación mensual para el primer domingo de cada mes a las 6:00 AM.

Tema principal: Gestión del sistema Guardium

Exportación de resultados (CSV, CEF, PDF)

Los procesos de flujo de trabajo pueden crear archivos CSV, CEF y PDF. Esta función exporta todos estos tipos de archivo que se encuentran en el sistema Guardium.

Los archivos CEF/CSV creados por procesos de flujo de trabajo también se pueden escribir en el syslog. Cuando esto sucede, estos archivos no están disponibles para su exportación como se describe aquí. Se debería acceder a estos archivos desde el syslog de otras formas.

Para exportar archivos CSV, CEF y PDF:

1. Abra Exportar resultados (archivos) pulsando Gestionar > Gestión de datos > Exportar resultados (archivos).
2. Elija una opción en los botones de selección Protocolos: SCP, FTP, Amazon S3 o Softlayer.
3. Para Host, especifique la dirección IP o nombre de host DNS del host que recibirá los archivos.
4. Para Directorio, identifique el directorio en el que se almacenarán los datos. La forma de especificar este directorio depende del protocolo que haya seleccionado.
    - Para FTP: Especifique el directorio relativo al directorio de inicio de la cuenta FTP.
    - Para SCP: Especifique el directorio como una vía de acceso absoluta.
5. Cambie el Puerto que se puede utilizar para enviar archivos a través de SCP y FTP. El puerto predeterminado para SSH, FTP y SFTP es 22. El puerto predeterminado para FTP es 21.
6. Para Nombre de usuario y Contraseña, especifique las credenciales del usuario que inicia sesión en la máquina host. Este usuario debe tener permisos de escritura/ejecución para el directorio especificado en el campo Directorio.
7. Utilice la sección Planificación para definir una planificación para ejecutar esta operación regularmente.
8. Pulse Guardar para guardar la configuración. El sistema intenta verificar la configuración enviando un archivo de datos de prueba a esa ubicación. Si la operación falla, aparece un mensaje de error.
9. Pulse Ejecutar una vez ahora para ejecutar la operación una vez.
10. Para verificar que los archivos se hayan exportado, marque Registro de agregación/archivado. Debería haber una actividad Enviar para cada archivo CSV o CEF exportado.

Para definir un separador predeterminado, abra el Perfil global pulsando Configuración > Herramientas y vistas > Perfil global.

Para especificar una etiqueta para que se incluya en todos los nombres de archivo, vaya a Herramientas > Creador de procesos de auditoría.
Nota:

El tamaño de mensaje máximo de syslog es 4000. Si los resultados de CSV superan este límite, se truncarán.

Establezca la codificación en UTF-8 independientemente de la aplicación que se utilice para leer los archivos .CSV. El conjunto de caracteres predeterminado de Excel es distinto y puede dañar los archivos .CSV. Además, cuando utilice Excel, importe el archivo .CSV y seleccione codificación UTF-8 en lugar de simplemente abrir el archivo y que Excel lo abra según la asociación de archivo.

Tema principal: Gestión del sistema Guardium

Exportar/Importar definiciones

Si tiene varios sistemas con requisitos idénticos o similares, y no utiliza Gestión central, puede definir los componentes que necesita en un sistema y exportar esas definiciones en otros sistemas, siempre y cuando esos sistemas tengan el mismo nivel de release de software.

Puede exportar un solo tipo de definición (por ejemplo, informes) cada vez. Cada elemento exportado puede causar que se exporten también otras definiciones referenciadas. Por ejemplo, un informe se basa siempre en una consulta, y también puede hacer referencia a otros elementos, como grupos de direcciones IP o periodos de tiempo. Todas las definiciones referenciadas (excepto los roles de seguridad) se exportan junto con la definición de informe. Sin embargo, sólo se exporta una copia de una definición si se hace referencia a esa definición en varios elementos exportados. Una exportación de políticas o consultas sólo exporta los grupos a los que hacen referencia las consultas o políticas exportadas. Anteriormente, una exportación de políticas o consultas exportaría todos los grupos.

Exportar/Importar definiciones

Exportar definiciones e Importar definiciones se utilizan para guardar y a continuación restaurar datos funcionales de un sistema Guardium determinado. Por ejemplo, esta función le permite crear un informe en un sistema Guardium y a continuación importar ese mismo informe en otro servidor que tenga instalada la misma versión de Guardium.
Nota: Esta función no es la misma que la copia de seguridad completa del servidor. Las copias de seguridad se deben seguir realizando y ejecutando de forma manual o planificada.
Exportar definiciones: Se utiliza para guardar y compartir valores funcionales definidos como por ejemplo informes/consultas, datos de CAS, datos de clasificador, etc. Los tipos de exportación se guardan en el PC como un tipo de archivo .sql.
Importar definiciones: Esta función se utiliza para importar las definiciones exportadas en los servidores que utilizan la misma versión de software de Guardium. Por ejemplo, si exporta definiciones de un sistema Guardium V10, puede importar esas definiciones sólo en otro sistema de la versión 10.

Nota:

- Cuando se exportan informes gráficos, los valores de los parámetros de presentación (colores, fonts, títulos, etc.) no se exportan. Cuando se importan, estos informes utilizan los valores de los parámetros de presentación predeterminados del sistema de importación.
- Los grupos suscritos no se exportan. Cuando se exportan definiciones que hacen referencia a grupos suscritos, el usuario debe asegurarse de que todos los grupos suscritos referenciados estén instalados en el dispositivo de importación (o Gestor central en un entorno federado).
- Los registros de Exportar/Importar definiciones tienen el mismo periodo de retención que los registros de actividad de la base de datos supervisada.
- Los comentarios no se incluyen en la exportación.
- Cuando se exportan a otro sistema definiciones de proceso de auditoría de ejecuciones planificadas (incluida la hora de planificación), el recuadro de selección ACTIVO del Creador de procesos de auditoría no está seleccionado (INACTIVO).

- Hora de inicio planificada de un proceso de auditoría definido en un dispositivo y exportado a otro dispositivo (no relacionado): En el caso de que esté definida la hora de inicio planificada original, se retiene. Si la hora de inicio planificada original no está definida (está vacía), la hora de inicio de planificación importada se establece en la hora a la que se ha importado.
- Cuando se exporta un origen de datos con un controlador de código abierto, el controlador de código abierto no se incluye en la exportación. El usuario debe subir primero el controlador de código abierto al sistema antes de importar la definición de origen de datos creada utilizándolo; de lo contrario, el controlador Data Direct se sustituirá por el controlador de código abierto cuando se importe.
- Las importaciones complejas de gran tamaño pueden tardar mucho tiempo y pueden superar la duración de la sesión del usuario. Si esto ocurre y la sesión excede el tiempo de espera, la importación continúa ejecutándose en segundo plano hasta que se completa.
- Cuando exporta la definición de políticas de clasificador, las clases de evaluación personalizadas asociadas con las políticas no se exportan con la definición. Para que las políticas importadas funcionen, se deben subir clases de evaluación por separado.
- La exportación/importación de definiciones entre distintos idiomas no funciona. Por ejemplo, si intenta exportar un archivo desde un sistema Guardium en chino simplificado e importar ese archivo en un sistema Guardium en inglés, esto dará un error.

Exportar a protocolo XACML

Guardium da soporte a la exportación de reglas de política a un archivo XACML, y a la importación de archivos XACML a otro sistema Guardium.

XACML (eXtensible Access Control Markup Language) es un lenguaje de política de control de accesos declarativo que se implementa en XML y un modelo de proceso que describe cómo interpretar las políticas.

Se utiliza la exportación/importación a XACML estándar como una interfaz bidireccional para transferir reglas de políticas entre Optim Designer y Guardium.

Optim Designer puede convertir valores de datos para diversos fines y de diversas formas. En el tiempo de ejecución de núcleo de Optim (z/OS y distribuido), esto se consigue mediante la invocación de funciones de privacidad de datos declaradas en correlaciones de columnas. En Optim Privacy esto lo especifica el usuario como la aplicación de una política de privacidad de datos en un atributo, referenciado por una entidad en un plan de acceso de datos.

Los clientes que han comprado ambos productos, Optim Privacy y Guardium, podrán exportar a XACML las políticas y la información de privacidad desde un producto e importarlos en el otro producto.

Nota: No se da soporte a importaciones de XACML desde versiones anteriores de Guardium.
Para exportar políticas de Guardium a XACML, siga estos pasos:

1. Pulse Gestionar > Gestión de datos > Exportar.
2. Seleccione Política en el menú Tipo.
3. Marque el recuadro de selección Exportar a archivo XACML.
4. Seleccione definiciones en el menú Definiciones para exportar.
5. Pulse Exportar.

Para importar un archivo XACML desde otro sistema Guardium u Optim Privacy, abra Importar definiciones pulsando Gestionar > Gestión de datos > Importar.

Importación de grupos

Cuando se importa un grupo que ya existe, se pueden añadir miembros, pero no se suprimirá ningún miembro.

Importación de alias

Cuando se importan alias, se pueden añadir alias nuevos, pero no se suprimirá ningún alias.

Propiedad de las definiciones importadas

Cuando se crea una definición, el usuario que la crea se guarda como propietario de esa definición. Esto significa que si no hay roles de seguridad asignados a esa definición, sólo el propietario y el usuario de administración tendrán acceso a ella.

Cuando se importa una definición, el propietario siempre cambia a admin.

Roles para definiciones importadas

Las referencias a roles de seguridad se eliminan de las definiciones exportadas. Por lo tanto, las definiciones importadas no tendrán roles asignados.

Usuarios de las definiciones importadas

Una referencia a un usuario en una definición exportada hace que la definición de usuario se exporte. Cuando se importan definiciones, las definiciones referenciadas se importan sólo si no existen en el sistema de importación. En otras palabras, las definiciones de usuario existentes nunca se sobrescriben. Esto tiene varias implicaciones, tal como se describe en Implicaciones de un rol y usuario duplicado.

Además, las definiciones de usuario importadas están inhabilitadas. Esto significa que los usuarios importados pueden recibir notificaciones por correo electrónico que se envían desde el sistema de importación, pero no pueden iniciar sesión en ese sistema, a menos que el administrador habilite esa cuenta.

Implicaciones de un usuario y grupo duplicado

Si un grupo referenciado por una definición exportada existe en el sistema de importación, la definición de ese grupo del sistema de exportación no se importará. Esto puede crear alguna confusión si el grupo no se utiliza para los mismos fines en ambos sistemas.

Si existe una definición de usuario existe en el sistema de importación, puede que no sea para la misma persona que está definida en el sistema de exportación. Por ejemplo, supongamos que en el sistema de exportación el usuario jdoe con la dirección de correo electrónico john_doe@aaa.com es un destinatario de la salida de una alerta exportada. Supongamos también que en el sistema de importación el usuario jdoe ya existe para una persona con la dirección de correo electrónico jane_doe@zzz.com. La definición de usuario exportada no se importa, y cuando se desencadena la alerta importada, se envía un correo electrónico a la dirección jane_doe@zzzx.com. En cualquiera de los dos casos, cuando no se importen roles de seguridad o definiciones de usuario, compruebe las definiciones en ambos sistemas para ver si hay diferencias. Si es así, realice los ajustes correspondientes a dichas definiciones.

Tipos de definición para la exportación

Tabla 1. Tipos de definición para la exportación

Se puede exportar	No se puede exportar
Alerta	Clase de alerta personalizada Un recuadro de selección en la pantalla Exportar definiciones excluirá miembros del grupo. Consulte la descripción en el elemento de línea Grupo.
Alias	Prueba de asesoramiento personalizada
Proceso de auditoría	Procedimiento de identificación personalizado
Proceso de descubrimiento automático	
Hosts de CAS	
Conjuntos de plantillas de CAS	
Proceso de clasificación	Regla de acceso
Política de clasificador	
Permiso de conexión de clase personalizada	
Dominio personalizado	
Tabla personalizada	
Origen de datos	
Tipo de suceso	
Grupo	Un recuadro de selección en la pantalla Exportar definiciones excluirá miembros del grupo. Este recuadro de selección sólo está visible para los conjuntos de datos que tienen grupos en algún lugar de la jerarquía de exportación (por ejemplo, la exportación de una alerta también incluye la consulta de la alerta y la consulta podría incluir grupos en las condiciones de consulta). Si la exportación del origen de datos no incluye grupos, el recuadro de selección no es visible. Cuando se establece este recuadro de selección, el archivo de exportación incluye grupos (si hay grupos enlazados a la definición exportada) pero los miembros de los grupos no se exportan. El recuadro de selección no está establecido de forma predeterminada, su estado no es persistente, y sólo se aplica a la exportación actual.
Plantilla con nombre	
Periodo (periodo de tiempo)	
Política (pero no una línea base incluida)	
Conjunto de privacidad	
Consulta	
Reproducir	
Informe	Un recuadro de selección en la pantalla Exportar definiciones excluirá miembros del grupo. Consulte la descripción en el elemento de línea Grupo.
Rol	
Asesoramiento de seguridad	
Usuario	
Correlación de base de datos de usuarios	
Permiso de base de datos de usuarios	
Jerarquía de usuarios	

Exportar definiciones

1. Abra el panel Exportar definiciones pulsando Gestionar > Gestión de datos > Exportar.
2. Seleccione una opción en el menú Tipo. El menú Definiciones para exportar se llenará con las definiciones del tipo seleccionado.
3. Seleccione todas las definiciones de este tipo que se exportarán.
   Nota: No exporte una definición de política cuyo nombre contenga comillas. Esa definición se puede exportar, pero no se puede importar. Para exportar una definición de este tipo, clónela, dé al clon un nombre que no contenga comillas y expórtelo.
4. Pulse Exportar. En función de los valores de seguridad del navegador, es posible que reciba un mensaje de aviso que le solicite si desea guardar el archivo o abrirlo mediante un editor.
5. Guarde el archivo exportado en una ubicación adecuada.

Importar definiciones

1. Abra el panel Importar definiciones pulsando Gestionar > Gestión de datos > Importar.
2. Pulse Examinar para localizar y seleccionar el archivo.
3. Pulse Subir. Se le notificará cuando la operación se complete y se mostrarán las definiciones contenidas en el archivo. Repita este paso para subir archivos adicionales.
4. Utilice el recuadro de selección Miembros de grupos totalmente sincronizados para establecer el comportamiento de cómo añadir nuevos miembros de grupo importados directamente o mediante otros conjuntos de datos como por ejemplo consultas o políticas. Si no se selecciona, los nuevos miembros que están en la importación se añadirán, pero los miembros que no están en la importación no se eliminarán. Si se selecciona, los miembros de grupo que no están en la importación se eliminarán. Utilice el botón Establecer como predeterminado junto al recuadro de selección para guardar el valor del recuadro de selección.
5. Pulse Importar este conjunto de definiciones para importar un conjunto de definiciones, o pulse Eliminar este conjunto de definiciones sin importar para eliminar el archivo subido sin importar las definiciones.

6. Se le solicitará que confirme una de las dos acciones.
   Nota: Una operación de importación no sobrescribe una definición existente. Si intenta importar una definición con el mismo nombre que una definición existente, se le notificará que el elemento no se ha sustituido. Si desea sobrescribir una definición existente con una definición importada, debe suprimir la definición existente antes de realizar la operación de importación.

Tema principal: Gestión del sistema Guardium

Interfaz distribuida

Utilice esta pantalla de configuración para definir la interfaz distribuida y subir el archivo de almacenamiento intermedio de protocolo (.proto) a la base de datos DIST_INT.

Desde esta base de datos, los metadatos de Dominio de consulta se crean automáticamente. Una vez que se han creado los metadatos, el usuario puede ir al Creador de dominios personalizados para modificar o clonar los datos y crear informes personalizados. Los datos de la interfaz distribuida utilizan almacenamientos intermedios de protocolo. Los almacenamientos intermedios de protocolo son un mecanismo flexible, eficiente y automatizado para la serialización de datos estructurados.

Para el canal de información universal de tipo 3, suba el archivo de definición de protocolo para la configuración de la base de datos DIST_INT pulsando Gestionar > Gestión de datos > Interfaz distribuida.

Nota: Pulse Mantenimiento para gestionar el tipo de motor de tabla y el índice de tabla. Los tipos de motor de tabla para las tablas de canal de información universal (InnoDB y MyISAM) aparecerán para todas las tablas de canal de información universal, ya que los datos almacenados en la base de datos interna de Guardium están basados en MYSQL. Consulte Correlación de datos externos para obtener más información sobre el mantenimiento de MyISAM e InnoDB.

Configurar la interfaz distribuida

1. Abra el Buscador de interfaces distribuidas pulsando Gestionar > Gestión de datos > Interfaz distribuida.
2. Pulse Nuevo para crear una nueva interfaz distribuida, o seleccione una interfaz distribuida existente en el Buscador de interfaces distribuidas y pulse Modificar o Suprimir.
3. Para ID de proveedor, especifique el ID del proveedor (por ejemplo, 20000).
4. Para Nombre de dominio, especifique el nombre del dominio que será seleccionable en el Creador de dominios personalizados.
5. Seleccione Incluido en la agregación
6. Para Nombre de archivo, pulse Examinar para seleccionar un archivo.
7. Pulse Aplicar para guardar esta configuración.
8. Cree un informe personalizado en el Creador de dominios personalizados. Abra el Creador de dominios personalizados pulsando Configuración > Herramientas y vistas > Creador de dominios personalizados.

Ejemplo de un archivo .proto

```
package bim;
option java_package = "com.ibm.infosphere.bim.proto";
option java_outer_classname = "BimEvent";
// NOTA: AssetID y Property_type (== Property name!) son series.
// Para AssetID, es más seguro utilizar un UUID porque proporciona un ID exclusivo mundial.
// Será la clave para la tabla de valores de métricas y propiedades actuales.
// por cada activo, por cada propiedad, habrá un único valor (recent, min, max, etc.)
message EventTypeID {
    required string eventType                   = 1; //p.ej. Cambio de esquema
}
message AssetID {
    required string assetId                     = 1;
}
message InfoPropertyID {
    required string assetId                     = 1;
    required string propertyName                = 2;
}
message MetricPropertyID {
    required string assetId                     = 1;
    required string propertyName                = 2;
}
message AssetRelationID {
    // Son ID "nativos" de activo
    required string sourceAssetId               = 1;
    required string targetAssetId               = 2;
}
message RelationPropertyID {
    required string assetRelationId             = 1;
    required string propertyName                = 2;
}
message Event {
    optional InnerEvent innerEvent              = 1;
}
message InnerEvent {
    // Común para todos los sucesos
    optional EventTypeID eventTypeId                = 1;
    optional string description                     = 2;
    optional string time                            = 3;
    optional string agentId                         = 4;
    // El suceso puede ser para info. de activo, o propiedad de métrica
    optional AssetInfoEvent assetInfoEvent          = 5;
    optional MetricPropertyEvent metricPropertyEvent  = 6;
    optional AssetRelationEvent  relationEvent      = 7;
    optional RuleEvent ruleEvent                    = 8;
}
message AssetInfoEvent {
    optional AssetID unique_key__               = 1;
    optional string assetType                   = 2;
    optional string assetName                   = 3;
    optional string gdm_server_ip               = 4;
```

```
    optional string gdm_service_name            = 5;
    repeated InfoProperty property              = 6;
}
message InfoProperty {
    optional InfoPropertyID unique_key__        = 1;
    optional string value                       = 2;
}
message MetricPropertyEvent {
    optional AssetID assetId                    = 1;
    repeated MetricProperty property            = 2;
}
message MetricProperty {
    optional MetricPropertyID unique_key__      = 1;
    optional AssetID assetId                    = 2;
    optional string stringValue                 = 3;
    optional double doubleValue                 = 4;

    enum Data_type {
        DOUBLE                                      = 1;
        LONG                                        = 2;
        INT                                         = 3;
        FLOAT                                       = 4;
        DATE                                        = 5;
        BOOLEAN                                     = 6; // la convención es almacenarlo
como 0 y 1 en double_value
        STRING                                      = 7; // almacenado en string_value
    }
        optional Data_type dataType                = 5;
    optional string unit                        = 6; // unidad del valor
}
message AssetRelationEvent {
    optional AssetRelationID unique_key__       = 1;
    required string relationshipType            = 2;
    repeated RelationshipProperty property      = 3;
    optional bool deleted                       = 4;
}
message RelationshipProperty {
    optional RelationPropertyID unique_key__    = 1;
    optional string value                       = 2;
}
message RuleEvent {
    optional string ruleName                    = 1;
    optional bool enabled                       = 2;
}
// --- Metadatos --- Todos los identificadores exclusivos se deben definir aquí
message Identifier {
    optional InfoPropertyID infoPropertyId                = 1;
    optional MetricPropertyID metricPropertyId            = 2;
    optional AssetID assetId                              = 3;
    optional AssetRelationID assetRelationId              = 4;
    optional RelationPropertyID relationshipPropertyId    = 5;
}
```

Tema principal: Gestión del sistema Guardium

Gestionar clases personalizadas

Suba y mantenga clases personalizadas utilizadas en alertas o evaluaciones. Gestione las clases personalizadas pulsando Configuración > Clases personalizadas.

Después de compilar una clase, debe subirse al sistema Guardium.

Subida de una clase personalizada

1. Puede subir una clase personalizada para alertas o evaluaciones. Suba una clase personalizada pulsando Configuración > Clases personalizadas, y a continuación Alertas > Subir o Evaluaciones > Subir
2. Especifique una descripción para la clase personalizada.
3. Pulse Examinar para localizar y seleccione el archivo de clase que desea subir.
4. Pulse Aplicar.

Actualización de una clase personalizada

1. Seleccione Configuración > Clases personalizadas y a continuación Alertas > Actualizar o Evaluaciones > Actualizar.
2. Seleccione la descripción de la clase que se actualizará.
3. Pulse Examinar para localizar y seleccionar el archivo de clase que se utilizará para la actualización.
4. Pulse Aplicar.

Supresión de una clase personalizada

1. Seleccione Configuración y a continuación Alertas > Suprimir o Evaluaciones > Suprimir
2. Seleccione la descripción de la clase que se suprimirá.
   Nota: No puede eliminar una clase que está utilizando algún otro componente (por ejemplo, la política instalada).
3. Pulse Suprimir.

Tema principal: Gestión del sistema Guardium

Subida de un archivo de claves

En condiciones excepcionales se debe subir un archivo de claves de Microsoft SQL Server al sistema Guardium para supervisar el tráfico cifrado de SQL Server.

No es necesario ningún archivo de claves si se ha instalado un S-TAP en SQL Server y se ha configurado para manejar el cifrado. Esta es la forma recomendada y más habitual de configurar un agente de S-TAP para MS SQL Server. Para determinar si un S-TAP está configurado para manejar el tráfico cifrado de MS SQL Server:

1. Abra el Control de S-TAP pulsando Gestionar > Supervisión de actividad > Control de S-TAP.
2. Expanda el panel Detalles para el agente de S-TAP en el host de MS SQL Server.
3. Verifique que la propiedad *Descifrado de TAP de SQL Server* se haya establecido en Sólo SSL o en Kerberos y SSL.
4. Si la propiedad *Descifrado de TAP de SQL Server* se ha establecido en Ninguna, se recomienda cambiar ese valor a Sólo SSL o Kerberos y SSL. Consulte Configurar S-TAP desde la interfaz gráfica de usuario para obtener información detallada sobre la configuración de S-TAP de Windows.
   Nota: Después de cambiar la propiedad *Descifrado de TAP de SQL Server*, debe reiniciar el servicio S-TAP y el servicio de supervisión MSSQL para que el cambio entre en vigor.

   Si por algún motivo no se le permite cambiar el valor Descifrado de TAP de SQL Server, utilice este procedimiento para subir un archivo de claves desde el servidor.

Si no se ha instalado ningún S-TAP, o si se ha instalado pero no está configurado para manejar el tráfico cifrado de SQL Server, es necesario un archivo de claves para supervisar el tráfico de SQL Server en las condiciones siguientes:

- Si el servidor se ha configurado utilizando la opción de forzar cifrado de protocolo.
- Si el servidor en un entorno de SQL Server 2005 utiliza sesiones de inicio de sesión cifradas con la autenticación mixta de SQL Server.

Dado que un solo sistema Guardium puede estar supervisando varias instancias de SQL Server, es posible que tenga que subir varios archivos de claves. Para subir un archivo de claves en el sistema Guardium:

1. Pulse Configuración > Herramientas y vistas > Subir archivo de claves.
2. Pulse Examinar para localizar el archivo de claves que desea subir.
   Nota: El nombre del archivo de claves debe ser el nombre de dominio completo de SQL Server. El archivo de clase no se puede renombrar, debe crearse con ese nombre.
3. Pulse Subir archivo de claves. Se le informará de los resultados de la operación.

Tema principal: Gestión del sistema Guardium

Claves públicas SSH

Utilice esta información para crear, modificar o eliminar una clave pública SSH.

1. Pulse Gestionar > Supervisión de actividad > Gestión de claves públicas SSH y realice una de las acciones siguientes:
   - Para crear una clave, pulse Nuevo.
   - Para generar una clase, pulse Generar.
   - Para modificar una clave, selecciónela en la lista y pulse Modificar.
   - Para eliminar una clave, selecciónela en la lista y pulse Eliminar.
2. Rellene la información adecuada en el panel Editar clave pública SSH y pulse Aplicar para guardar.

Tema principal: Gestión del sistema Guardium

Cómo instalar un certificado de dispositivo para evitar un reto de certificado SSL del navegador

Utilice los mandatos de CLI de IBM Security Guardium para crear una solicitud de firma de certificado (CSR) e instalar certificados de servidor, autoridad emisora de certificados o vías de acceso de confianza en el sistema Guardium.

Acerca de esta tarea

Elimine las pantallas de aviso de error de certificado que indiquen:

```
Hay un problema con el certificado de seguridad de este sitio web.  El certificado de seguridad que presenta este sitio web se ha emitido para la dirección de otro sitio web. Los problemas de certificados de seguridad pueden indicar un intento de engaño o de interceptar los datos que se envían a un servidor.
```

Consulte Mandatos de CLI de certificado para obtener más información sobre todos los mandatos de certificado.

Nota: Un requisito previo es que debe proporcionar un certificado público de una autoridad emisora de certificados que utilizará para firmar los certificados (Verisign, Thwate, Geotrust, GoDaddy, Comodo, internos de la empresa, etc.).
Nota: Guardium no proporciona servicios de autoridad emisora de certificados y no proporcionará sistemas con certificados distintos al que se instala de forma predeterminada. Un cliente que desee su propio certificado deberá ponerse en contacto con una autoridad emisora de certificados externa.
Nota: Si el certificado no es autofirmado, DEBE obtener también el certificado público para cada firmante hasta el nivel inferior (por ejemplo, el certificado autofirmado). Puede utilizar el mandato openssl x509 -in t.pem -text -noout para mostrar el contenido de un certificado x509.

Procedimiento

1. Tenga disponible el certificado público de la autoridad emisora de certificados que utilizará para firmar los certificados (de Verisign, Thwate, Geotrust, GoDaddy, Comodo, internos, etc).
2. Inicie sesión en la CLI en el sistema Guardium individual en el que desea tener un certificado firmado.

   Antes de ejecutar el mandato, obtenga el certificado adecuado (en formato PEM, no en formato binario) de la autoridad emisora de certificados, y copie el certificado, incluidas las líneas Begin y End, en el portapapeles.

3. Especifique el mandato store certificate keystore. Se mostrará el siguiente indicador de solicitud:

   ```
   ¿Cuál es el alias de una sola palabra que podemos utilizar para identificar de forma exclusiva este certificado?
   ```

   Especifique un nombre de una sola palabra para el certificado y pulse Intro.

Se mostrarán las instrucciones siguientes:

```
Pegue su certificado de autoridad emisora de certificados, en formato PEM. Incluya las líneas BEGIN y END y a continuación
pulse CTRL-D.
```

Pegue el certificado con formato PEM en la línea de mandatos y a continuación pulse CRTL-D. Se le informará del éxito o error de la operación de almacenamiento.

Ahora la autoridad emisora de certificados con la que firmará está establecida como de confianza en el sistema Guardium.

4. A continuación, en el indicador de mandatos de CLI, escriba: `create csr gui`.

   Rellene la información solicitada. Si el CN (nombre común) del certificado no está establecido en el nombrehost.dominio del sistema, se producirán errores de certificado del navegador.

   No hay parámetros, pero se le solicitará que proporcione la unidad organizativa (OU), el código de país (C), etc. Asegúrese de especificar correctamente esta información. La última solicitud es la siguiente:

   ```
   ¿Qué algoritmo de cifrado se debería utilizar (1=DSA o 2=RSA)?
   ```

   El algoritmo de firma digital, o DSA, es un estándar de proceso de información federal (FIPS) para firmas digitales. RSA es un criptosistema de clave pública que implica la generación de claves, el cifrado y el descifrado. El algoritmo de cifrado predeterminado es RSA.

   Cuando se ha respondido a la última solicitud, el sistema muestra una descripción de la solicitud, seguida de la propia solicitud, y seguida finalmente por instrucciones adicionales. Por ejemplo:

   ```
   This is the generated CSR: Certificate Request: Data: Version: 0 (0x0) Subject: C=US, ST=MA, L=Littleton, O=XYZCorp,
   OU=Accounting, CN=g2.xyz.com -----BEGIN NEW CERTIFICATE REQUEST-----
   MIICWjCCAhcCAQAwVDELMAkGA1UEBhMCVVMxEDAOBgNVBAgTB1dhbHRoYW0xETAPBgNVBAoTCEd1
   YXJkaXVtMRUwEwYDVQQLEwxndWFyZGl1bS5jb20xCTAHBgNVBAMTADCCAbgwggEsBgcqhkjOOAQB
   MIIBHwKBgQD9f1OBHXUSKVLfSpwu7OTn9hG3UjzvRADDHj+AtlEmaUVdQCJR+1k9jVj6v8X1ujD2
   y5tVbNeBO4AdNG/yZmC3a5lQpaSfn+gEexAiwk+7qdf+t8Yb+DtX58aophUPBPuD9tPFHsMCNVQT
   WhaRMvZ1864rYdcq7/IiAxmd0UgBxwIVAJdgUI8VIwvMspK5gqLrhAvwWBz1AoGBAPfhoIXWmz3e
   y7yrXDa4V7l5lK+7+jrqgvlXTAs9B4JnUVlXjrrUWU/mcQcQgYC0SRZxI+hMKBYTt88JMozIpuE8
   FnqLVHyNKOCjrh4rs6Z1kW6jfwv6ITVi8ftiegEkO8yk8b6oUZCJqIPf4VrlnwaSi2ZegHtVJWQB
   TDv+z0kqA4GFAAKBgQCONsEB4g4/limbHkuZ5YnLn9CGM3a2evEnqjXZts4itxeTYwPQvdkjdSmQ
   kaQlBxmNUsZOJZrq5nC5Cg3X9spa+BzFr+PgR/5zka17nHcxKXCjVjLk451L67KllXv61TUfv/bU
   PKmiaGKDttsP2ktG4dBFXQdICJEGo0aNFCYn6qAAMAsGByqGSM44BAMFAAMwADAtAhUAhHTY5z9X NiBAuyAC9PS4GzleYakCFF2kcfxfjX1BFy5I228XWMAU0N95
   -----END NEW CERTIFICATE REQUEST-----
   ```

   Nota: Para el nombre común (CN), utilice el nombre de host en formato FQDN (nombre de dominio completo). No obstante, si se conecta a la interfaz gráfica de usuario normalmente utilizando el nombre de host abreviado (por ejemplo, system1) en lugar de FDQN (system1.us.ibm.com), recibirá un error de certificado "Discrepancia de dirección". Deberá cambiar CN=system1 o conectarse con https://system1.us.ibm.com:8443/sqlguard para utilizar el certificado.
   Nota: El código de país debe tener 2 letras.
   Nota: El tamaño de clave puede ser 1024 o 2048.
5. Copie y pegue el hash generado de ---Begin CSR---- a ---End CSR--- en un documento de texto. A continuación envíelo a su autoridad emisora de certificados para que ellos le devuelvan la clave firmada.

   Antes de continuar, compruebe la línea del asunto para verificar que ha especificado correctamente la información de la empresa. A partir de este punto, utilice el procedimiento que utilizaría normalmente para obtener un certificado de servidor de su autoridad emisora de certificados.

   Nota: • Cuando envíe la solicitud a su autoridad emisora de certificados, asegúrese de que el certificado esté en el formato PEM PKCS#7.
6. La autoridad emisora de certificados firma la solicitud de firma de certificado y le devuelve su clave firmada.
7. A continuación, vuelva al indicador de solicitud de la CLI en el sistema Guardium y tenga disponible una clave firmada de la autoridad emisora de certificados. Especifique lo siguiente: store certificate gui.

   Especifique el mandato exactamente tal como se muestra. Recibirá la siguiente información y se le solicitará lo siguiente:

   Pegue su nuevo certificado de servidor, en formato PEM.

   Incluya las líneas BEGIN y END y a continuación pulse CTRL-D.

   Pegue el certificado con formato PEM en la línea de mandatos y a continuación pulse CRTL-D. Se le informará del éxito o error de la operación de almacenamiento.

   ```
   -----BEGIN CERTIFICATE----- MIIDvTCCAqegAwIBAgIBATALBgkqhkiG9w0BAQUwcjELMAkGA1UEBhMCVVMxEzAR
   BgNVBAgTCldhc2hpbmd0b24xDzANBgNVBAcTBllha2ltYTEMMAoGA1UEChMDSUJN
   MRUwEwYDVQQLEwxHdWFyZGl1bURlbW8xGDAWBgNVBAMTD0d1YXJkaXVtRGVtb19D
   QTAeFw0xMTAzMjUxNTM1MTRaFw02OTEyMzEyMzU5NTlaMHIxCzAJBgNVBAYTAlVT
   MRMwEQYDVQQIEwpXYXNoaW5ndG9uMQ8wDQYDVQQHEwZZYWtpbWExDDAKBgNVBAoT
   A0lCTTEVMBMGA1UECxMMR3VhcmRpdW1EZW1vMRgwFgYDVQQDEw9HdWFyZGl1bURl
   bW9fQ0EwggEgMAsGCSqGSIb3DQEBAQOCAQ8AMIIBCgKCAQEAw08aZVJNdnC69LR6
   YtvHO+KbsqA89vCezLw7xmEa7F6+io0NofIFX7b7FvSkxzx1SO4eStaQSTDBxOGk
   mqK2vk3VeJk9+lItofUuQXl1CZ1R4wQPMRfaWgELt+t94XB3Y1zmI68vwfr1fB32
   u3Yjpt4aq27sTMrjEqZIyDqQ7hQ1tpMtoBUqNi54wN+OJjhtpNYDAkCHs+3NPqXE
   6HeL7W5X6PJ+YCyyZiXeqQ+T8qdpH0KDVJGJLGX1YC+0WnQz/S2kaaRfxe6Nhe6q
   YeYaD09tlWkVrZQm8a76SDULjzjrQ4wNoTJu17JQk7Uc835RE/bF5WMsaN5HGs3s
   9zP3uwIDAQABo2QwYjAPBgNVHRMBAf8EBTADAQH/MA8GA1UdDwEB/wQFAwMHBgAw
   HQYDVR0OBBYEFINmKThm8tA+Z8cyFC7MOZ7v398SMB8GA1UdIwQYMBaAFINmKThm
   8tA+Z8cyFC7MOZ7v398SMAsGCSqGSIb3DQEBBQOCAQEAcXttcJwy1aowq9wtJksK
   q6n6laEFR38i+pLJ6kArjoJGP5WxFdaYcDQr5cAw2Q6YFZvQGaYAqiSS6ezF20PT
   3BrrP+Mg/SK8jgPvM0ekodmpr385iQqSDneTTwPPrIaQBrrtb2510wHSEyiVcRRI
   4vn3ktVahjiSMD92bfmZilPYQ51pD0jFgGFFRvekulPWGWv7iuCT+alCM99/76xR
   uWrRc7cxypfxK1yymptizZVrxLHS47VVoXzmZ7yO3kfhhdZbBmoXg1MDM82rVdnp
   WVQdlSasn8deHaVG//RsCrWx4PxN8TVIDGbfh0nWRYU4zPORvWst3fa+h9B2W55z /A== -----END CERTIFICATE-----
   ```

8. Para el paso final, reinicie la interfaz de usuario mediante el mandato restart gui.

   Ahora ha instalado correctamente un certificado para una unidad de Guardium. Repita los pasos para cada uno de los sistemas Guardium locales.

Tema principal: Gestión del sistema Guardium

Autosupervisión

La solución Guardium se supervisa a sí misma para minimizar las interrupciones y corregir automáticamente los problemas siempre que sea posible.

Guardium utiliza un enfoque triple para asegurarse de que está disponible, funciona correctamente y no se ha manipulado, y alerta a los usuarios de los problemas:

- Informes: Ya sean de texto o gráficos, los informes se encuentran en el núcleo de la solución Guardium. Mediante la utilización del Generador de consultas y del Creador de informes de Guardium, un usuario puede informar de forma efectiva sobre cualquiera de los datos de autosupervisión recopilados en todas las entidades y todos los dominios asociados. Muchos de los informes predefinidos se pueden mejorar mediante esfuerzos más detallados para proporcionar niveles de granularidad más altos. Se ha creado un creador de consultas específico (VA Test Tracking) para informar sobre las pruebas que están disponibles para los asesoramientos de seguridad.
- Alertas: Además de crear informes, un usuario puede definir una alerta para estos informes gracias a umbrales definidos, que indican excepciones o infracciones de regla de política. Estas alertas pueden ser en tiempo real o se pueden determinar mediante el análisis histórico. A continuación, estas alertas pueden desencadenar una notificación a los usuarios mediante SMTP, SNMP, syslog o una clase Java™ personalizada.
- Programa de utilidad de autosupervisión: Guardium ha implementado un servicio de daemon de autosupervisión interno (que está siempre en ejecución) en los recopiladores y agregadores que se activa cada 5 minutos y realiza una exploración del sistema, comprobando si los componentes tienen la configuración óptima, la eficacia operativa y, si es necesario, las reparaciones. Por ejemplo, si el programa de utilidad encuentra el servidor web inactivo, en primer lugar validará un cierre completo del servicio, lo reiniciará y a continuación alertará a un usuario administrativo.

Componentes supervisados

Tabla 1. Componentes supervisados

Componentes	Cómo acceder
Sistema Espacio de disco(% lleno)	Gestionar > Vista de sistema > Supervisor del sistema Alerta: Puede utilizar las consultas y alertas de correlación, utilizando el dominio Almacenamiento intermedio de sniffer y la entidad Uso de almacenamiento intermedio de sniffer para crear alertas
Carga de CPU Tiempo de actividad y rearranques Uso de memoria Motor de supervisión (sniffer) - Estado: activo/inactivo/colgado/sobrecargado Uso de CPU Uso de memoria Sobrecarga y retardos (colas)	Informes > Informes operativos de Guardium > Supervisor del uso de almacenamiento intermedio Alerta: Puede utilizar las consultas y alertas de correlación, utilizando el dominio Almacenamiento intermedio de sniffer y la entidad Uso de almacenamiento intermedio de sniffer para crear alertas
Inicios de sesión fallidos	Gestionar > Vista de sistema > Supervisor del sistema. Alerta: puede utilizar las consultas y alertas de correlación, utilizando el dominio Inicio de sesión de Guardium y la entidad Inicios de sesión de usuarios de Guardium para crear alertas.
Solicitudes perdidas	Gestionar > Informes > Supervisión de actividad > Solicitudes descartadas Alerta: Puede utilizar las consultas y alertas de correlación, utilizando el dominio Excepciones y la entidad Excepciones para crear alertas.
Cambio en patrones de datos	Informes > Informes operativos en tiempo real > Alerta Valores modificados: Vea Visualización de una definición de proceso de auditoría para alerta: Cambios de origen de datos - alerta sobre cualquier cambio de origen de datos
Velocidades de paquetes Velocidades de solicitudes Datos ignorados	Informes > Informes operativos de Guardium > Supervisor de uso de almacenamiento intermedio Alerta: Puede utilizar las consultas y alertas de correlación, utilizando el dominio Almacenamiento intermedio de sniffer y la entidad Uso de almacenamiento intermedio de sniffer para crear alertas
Excepciones de trabajos planificados	Informes > Informes operativos de Guardium > Excepciones de trabajos planificados, o vea Informes de administración predefinidos: Alerta: Puede utilizar las consultas y alertas de correlación, utilizando el dominio Excepciones y la entidad Tipo de excepción para crear alertas.
Estado de procesos de auditoría	Informes > Informes operativos de Guardium > Número de procesos de auditoría activos, o vea Informes de administración predefinidos. Alerta: Puede utilizar las consultas y alertas de correlación, utilizando el dominio Proceso de auditoría y la entidad Proceso de auditoría para crear alertas.
Cambios del motor de inspección	Informes > Supervisión de actividad > Historial de cambios de configuración de S-TAP Alerta: Vea Visualización de una definición de proceso de auditoría para alerta: Motores de inspección y S-TAP - alerta sobre cualquier actividad relacionada con la configuración de S-TAP y el motor de inspección
Actividad de usuarios de Guardium - Iniciar sesión/Cerrar sesión	Informes > Informes operativos de Guardium > Inicios se sesión en Guardium, o vea Informes de administración predefinidos Alerta: Puede utilizar las consultas y alertas de correlación, utilizando el dominio Inicio de sesión de Guardium y la entidad Inicio de sesión de SQL Guard para crear alertas

Componentes	Cómo acceder
Inicios de sesión fallidos	Informes > Informes operativos de Guardium > Inicios se sesión en Guardium, o vea Informes de administración predefinidos Alerta: Vea Visualización de una definición de proceso de auditoría para alerta: Inicios de sesión fallidos en Guardium - alerta si tiene más de 5 inicios de sesión fallidos en los últimos 11 minutos, o seleccione Herramientas > Creación de informes > Título de informe desplegable: Inicios de sesión de Guardium, consulte Informes para obtener información adicional
Seguimiento de auditoría de actividad de usuario	Informes >Informes operativos de Guardium > Seguimiento de auditoría de actividad de usuario, o consulte Informes de administración predefinidos Alerta: Puede utilizar las consultas y alertas de correlación, utilizando el dominio Actividad de Guardium y la entidad Auditoría Actividad de usuario de SQL Guard para crear alertas. Nota: La actividad de usuario incluye aquellas instancias en las que un usuario cambia al shell de root, proporcionando un registro de su actividad de root.
Creación/Supresión de usuarios/roles	Informes >Informes operativos de Guardium > Seguimiento de auditoría de actividad de usuario, o consulte Informes de administración predefinidos Alerta: Consulte Visualización de una definición de proceso de auditoría para alerta: Guardium - Añadir/Eliminar usuarios - alerta sobre cualquier adición o eliminación de usuario de Guardium
Supervisión de permisos	Informes > Informes operativos de Guardium > Usuarios de Guardium, Roles de Guardium o Aplicaciones de Guardium Alerta: Puede utilizar las consultas y alertas de correlación, utilizando el dominio Aplicación y la entidad Datos de aplicación para crear alertas.
Información de S-TAP (Gestor central)	Informe: Consulte Informes de S-TAP. En un Gestor central, está disponible un informe adicional, Información de S-TAP. Este informe supervisa los S-TAP de todo el entorno. Suba estos datos utilizando el Creador de tablas personalizadas. Este informe es el resultado de la subida de datos utilizando orígenes remotos en un gestor central y utilizando esos datos para ver una vista consolidada de los S-TAP. Información de S-TAP es un dominio personalizado predefinido que contiene la entidad Información de S-TAP y no es modificable como el dominio Titularidad.

Proceso Nanny de Guardium

Nanny de Guardium es un proceso interno que supervisa los recursos críticos del sistema y, a continuación, alerta cuando surgen problemas potenciales. Las alertas de Nanny van a syslog, se pueden reenviar y enviar como correos electrónicos al administrador y, en algunos casos, llevar a cabo acciones correctivas.

Nanny observa los principales componentes y recursos críticos del sistema Guardium, garantizando su disponibilidad y fiabilidad. Estos recursos y componentes incluyen:

- Supervisión del servicio web - el puerto de servicio (valor predeterminado 8443) no responde o el servicio tomcat no está activo
  - Mensaje de syslog
  - administración de correo
  - emitirá reinicios del servicio web
- Actividad del motor de inspección - sniffer sobrecargado, no responde
  - Mensaje de syslog
  - administración de correo
  - Soporte de Guardium de correo (opcional)
  - intentará solucionarlo reiniciando el sniffer en determinadas condiciones
  - intentará regenerar el sniffer si el proceso termina
- Utilización de espacio de disco - alertas cuando > 75 % en las particiones críticas
  - Mensaje de syslog
  - administración de alertas
  - realizará una acción preventiva con la limpieza de archivos temporales cuando más de 95 %
- Error de inicio de sesión (ssh) en el dispositivo - comprueba los mensajes y alertas del daemon ssh en caso de intentos de inicio de sesión fallidos
  - administración de correo (ya está en syslog)
- Supervisar base de datos interna (TURBINE) - verifica si el servicio está activo, estado y supervisión de utilización de capacidad
  - Mensaje de syslog
  - administración de correo
  - reinicio del servicio
- Utilización del sistema de archivos - cada cinco minutos, Nanny.pl comprueba el sistema de archivos en /var, alerta de aviso cuando > 75 % en el directorio /var, alerta crítica y los servicios se detienen cuando > 90 % en el directorio /var
  - Mensaje de syslog
  - administración de alertas
  - Se requiere limpieza del administrador, utilizando mandatos de CLI: show filesystem usage, clear filesystem dir y restart stopped_services

- Cómo supervisar el sistema Guardium mediante alertas
  Supervise la capacidad, el rendimiento y la disponibilidad del sistema IBM Security Guardium utilizando una combinación de alertas de correlación personalizadas e incorporadas.
- Supervisión con SNMP
  Hay un agente SNMP instalado en los sistemas Guardium, y se proporciona acceso de sólo lectura utilizando el nombre de comunidad SNMP de guardiumsnmp.
- Supervisor de consultas en ejecución
  El Supervisor de consultas en ejecución muestra el estado de las consultas de usuario activas, y le permite establecer un valor de tiempo de espera para todas las consultas de informe/supervisor.

Tema principal: Gestión del sistema Guardium

Cómo supervisar el sistema Guardium mediante alertas

Supervise la capacidad, el rendimiento y la disponibilidad del sistema IBM Security Guardium utilizando una combinación de alertas de correlación personalizadas e incorporadas.

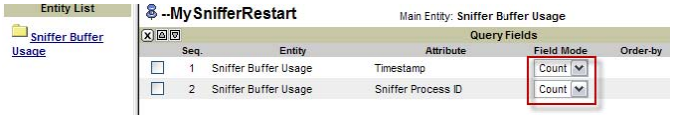
Alerte a los usuarios sobre problemas que pueden afectar al rendimiento del sistema como, por ejemplo: la utilización de CPU, el espacio de disco de base de datos, STAP inactivos y situaciones sin tráfico.

El dominio Uso de almacenamiento intermedio de sniffer es la base de la mayoría de las alertas siguientes.

Alerta de reinicio de sniffer

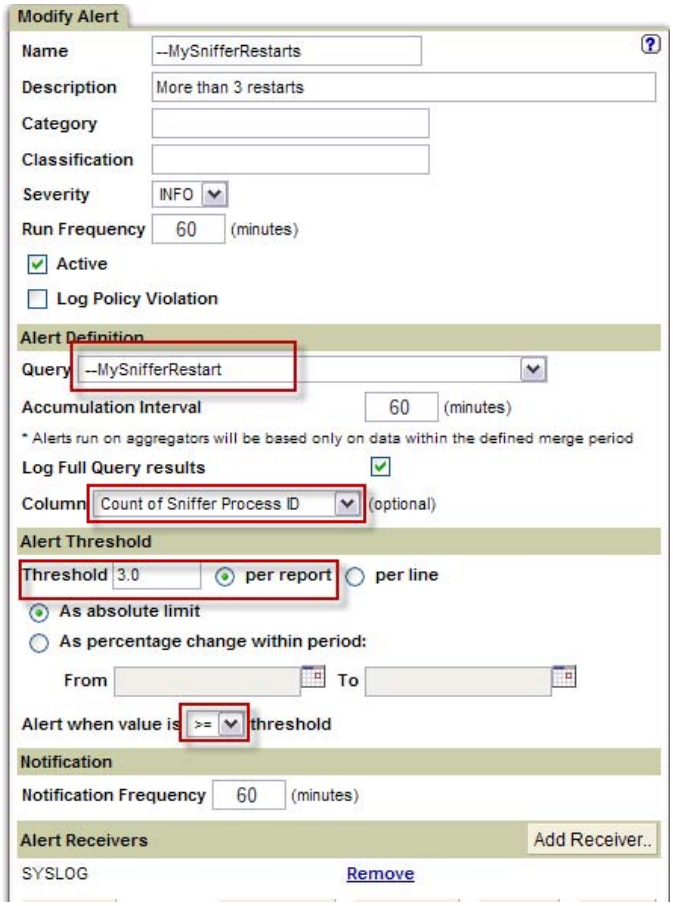
Se enviará una alerta si el sniffer de un recopilador se ha reiniciado al menos tres veces en una hora.

Cree una consulta utilizando el dominio Uso de almacenamiento intermedio de sniffer con las columnas y campos que se muestran – sin condiciones.



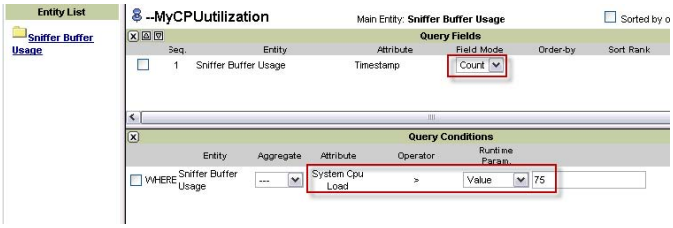
Este es un ejemplo de la salida de la consulta:

Defina la alerta.



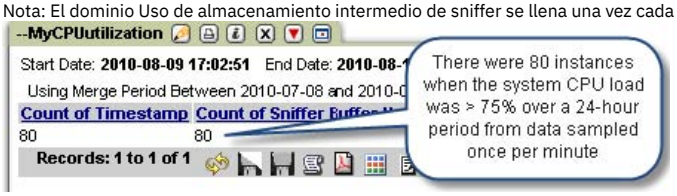
Alta utilización de CPU

Utilizando el dominio Uso de almacenamiento intermedio de empresa, cree una alerta para supervisar la utilización de CPU del sistema. A continuación se muestra un ejemplo de una consulta para la utilización de CPU que supera el 75 %.

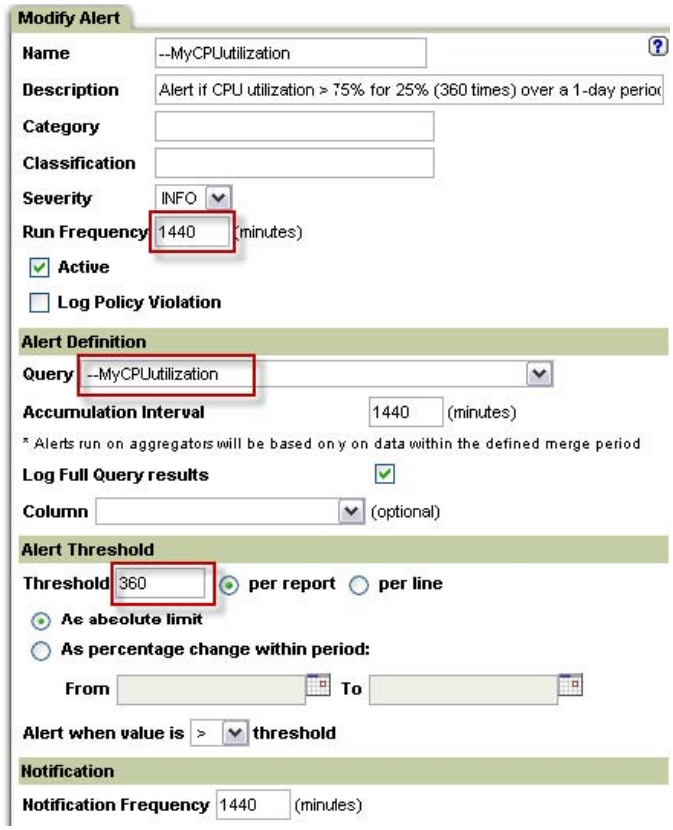


A continuación, la alerta se configurará para que se active sólo si la utilización se supera 360 veces en un periodo de 24 horas, por ejemplo, el 25 % del día.

Nota: El dominio Uso de almacenamiento intermedio de sniffer se llena una vez cada minuto, así que hay 1440 entradas en un periodo de 24 horas.



Para definir la alerta, pulse Proteger > Detección de intrusión en base de datos > Creador de alertas.

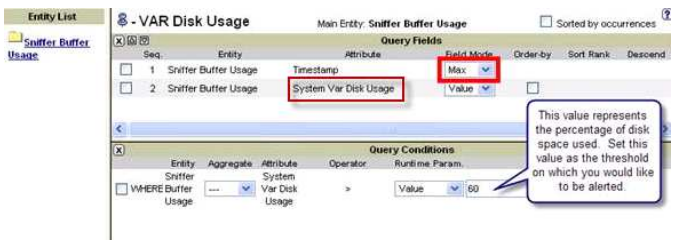


Alertas de espacio de disco de base de datos

Utilice el Creador de consultas para crear dos informes (que son similares) y dos alertas, una para el recopilador y la otra para el agregador, ya que el tamaño de base de datos es fijo en el recopilador pero dinámico en el agregador (hasta el tamaño de la partición var).

Alerta de espacio de disco de agregador

1. Cree una nueva consulta con Uso de almacenamiento intermedio de sniffer como la entidad principal.
2. Configure los campos y condiciones.

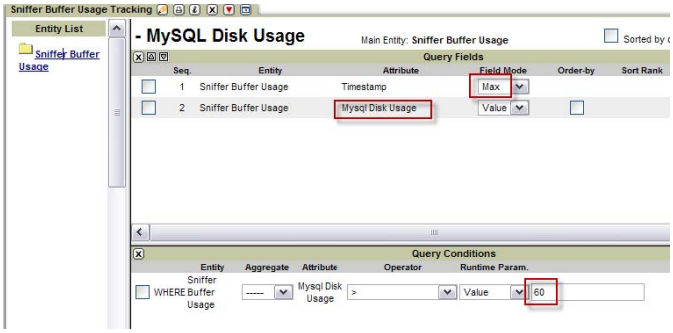


1. Configure una nueva alerta en el Creador de alertas. Abra el Creador de alertas pulsando Proteger > Detección de intrusión en base de datos > Creador de alertas.

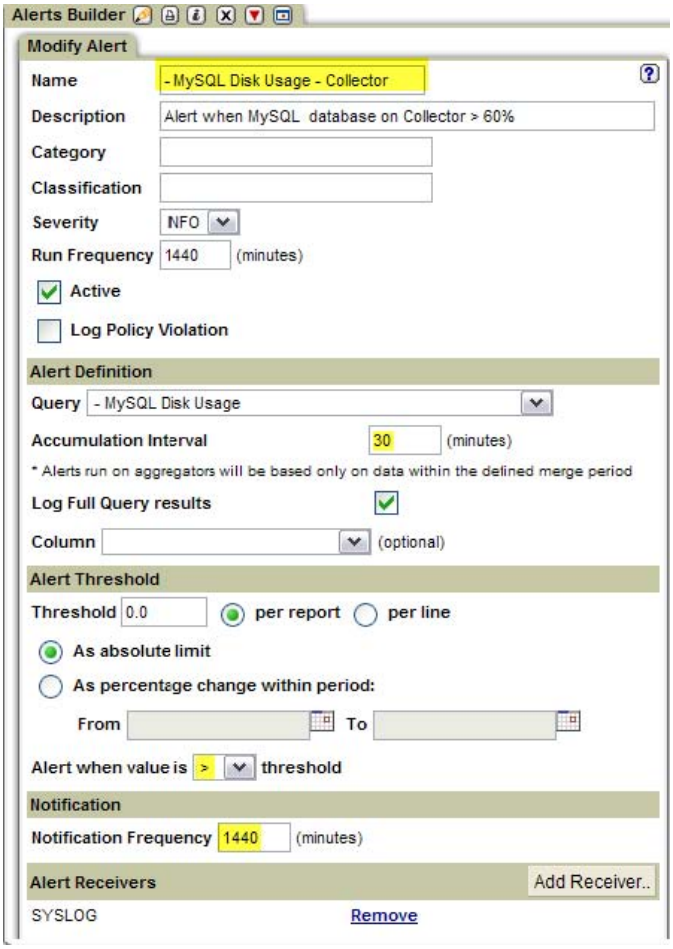
Alerta de espacio de disco de recopilador

Repita los pasos anteriores para crear una alerta para supervisar el espacio de disco en los recopiladores.

1. Cree una consulta.



1. Utilice el Creador de alertas para configurar una nueva alerta.



Alertas de error de importación, fusión (agregación), Archivado o copia de seguridad de datos

Es una alerta incorporada que se debe activar y planificar.

Alertas de S-TAP inactivo

Es una alerta incorporada que se debe activar y planificar.

Para los STAP configurados con un recopilador primario y un recopilador secundario, si el STAP no se puede comunicar con el primario (por ejemplo, debido a problemas de red), realizará la sustitución por anomalía al secundario. A menos que el recopilador primario anterior pueda ejecutar ping al STAP, generará una alerta de STAP inactivo.

Nota: Los STAP en una configuración de clúster pueden generar alertas falsas si no están configurados correctamente.

Alertas de sin tráfico

Es una alerta incorporada que se debe activar y planificar.

Esta alerta comprueba el tráfico de un motor de inspección activo, del que el recopilador ha recibido anteriormente tráfico, Y el tráfico que procesa la política. Si no se cumplen ambas condiciones en 48 horas, se generará una alerta.

Supervisión de aplicación mediante informes ad hoc

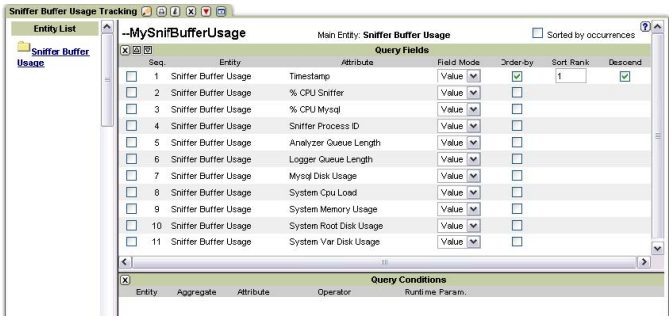
Como regla general, evite invocar consultas/informes ad hoc en el recopilador con plazos de tiempo mayores a 1 hora. Las consultas grandes o de larga ejecución se deberían invocar en el agregador y es mejor planificarlas utilizando el proceso de auditoría.

Se deben planificar los dos informes siguientes, desde el Gestor central, para ejecutarse semanalmente en cada recopilador.

Nota: También es necesario planificar estos informes individualmente en CADA agregador.

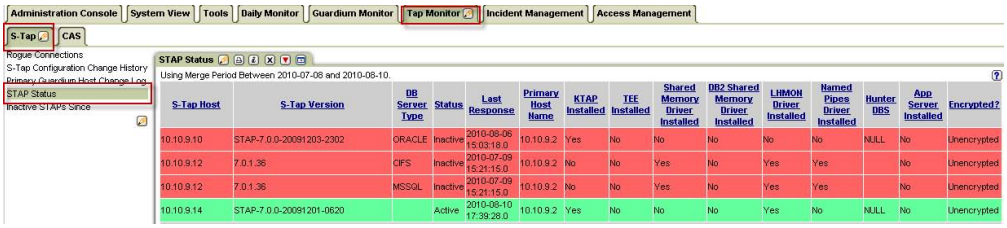
Informe Uso de almacenamiento intermedio de sniffer personalizado

Utilizando el dominio Uso de almacenamiento intermedio de sniffer, cree un informe con los campos siguientes:



Informe Estado de STAP

Este informe muestra los parámetros clave para TODOS los STAP y motores de inspección de un determinado recopilador. El informe no se puede modificar pero se puede ejecutar en cada recopilador, o desde el Gestor central que apunta a cada uno de los recopiladores, o planificar mediante el proceso de auditoría en cada recopilador.



Tema principal: Autosupervisión

Supervisión con SNMP

Hay un agente SNMP instalado en los sistemas Guardium, y se proporciona acceso de sólo lectura utilizando el nombre de comunidad SNMP de guardiumsnmp.

Al realizar consultas, un valor de -1 (menos uno) indica un NULL en la base de datos. La tabla al final de esta sección lista los OID de SNMP disponibles.

Ejemplos de SNMP

En una sesión de Unix, puede visualizar la información de SNMP de Guard de SQL mediante los mandatos snmpget o snmpwalk. (Utilice snmpget -h o snmpwalk -h para ver la sintaxis de los mandatos.) Hay disponibles varios paquetes de software basado en la interfaz de usuario para visualizar la información de SNMP. Estas alternativas no se describen aquí.

Tabla 1. Ejemplos de SNMP

Ejemplos de SNMP
Espacio de disco utilizado y disponible:
> snmpget -v 2c -c guardiumsnmp a1.corp.com UCD-SNMP-MIB::dskAvail.1
UCD-SNMP-MIB::dskAvail.1 = INTEGER: 1043856
> snmpget -v 2c -c guardiumsnmp a1.corp.com UCD-SNMP-MIB::dskUsed.1
UCD-SNMP-MIB::dskUsed.1 = INTEGER: 914856
Para listar la memoria total y la memoria utilizada:
> snmpget -v 2c -c guardiumsnmp a1.corp.com
HOST-RESOURCES-MIB::hrStorageSize.101
HOST-RESOURCES-MIB::hrStorageSize.101 = INTEGER: 2067352
> snmpget -v 2c -c guardiumsnmp a1.corp.com HOST-RESOURCES-MIB::hrStorageUsed.101
HOST-RESOURCES-MIB::hrStorageUsed.101 = INTEGER: 1017548

Ejemplos de SNMP
Para listar la memoria disponible:
> snmpwalk -v 2c -c guardiumsnmp a1.corp.com memAvailReal
UCD-SNMP-MIB::memAvailReal.0 = INTEGER: 1049564
Para listar los valores relacionados con el uso de CPU:
> snmpwalk -v 2c -c guardiumsnmp a1.corp.com ssCpuRawUser
UCD-SNMP-MIB::ssCpuRawUser.0 = Counter32: 89240
> snmpwalk -v 2c -c guardiumsnmp a1.corp.com ssCpuRawSystem
UCD-SNMP-MIB::ssCpuRawSystem.0 = Counter32: 195310
> snmpwalk -v 2c -c guardiumsnmp a1.corp.com ssCpuRawNice
UCD-SNMP-MIB::ssCpuRawNice.0 = Counter32: 11
Nota: La suma de los números de RawUser, RawSystem y RawNice proporciona una buena aproximación al uso total de CPU.
> snmpwalk -v 2c -c guardiumsnmp a1.corp.com ssCpuRawIdle
UCD-SNMP-MIB::ssCpuRawIdle.0 = Counter32: 26734332

OID de SNMP de Guardium

Tabla 2. OID de SNMP de Guardium

OID de SNMP	Descripción
.1.3.6.1.4.1.2021.9.1.7.1 UCD-SNMP-MIB::dskAvail.1	Espacio de disco disponible en el directorio /
.1.3.6.1.4.1.2021.9.1.7.2 UCD-SNMP-MIB::dskAvail.2	Espacio de disco disponible en el directorio /var
.1.3.6.1.4.1.2021.9.1.8.1 UCD-SNMP-MIB::dskUsed.1	Espacio de disco utilizado en el directorio /
.1.3.6.1.4.1.2021.9.1.8.2 UCD-SNMP-MIB::dskUsed.2	Espacio de disco utilizado en el directorio /var
.1.3.6.1.2.1.25.2.3.1.5.1 HOST-RESOURCES-MIB::hrStorageSize.1	Memoria total disponible
.1.3.6.1.2.1.25.2.3.1.6.1 HOST-RESOURCES-MIB::hrStorageUsed.1	Memoria en uso
.1.3.6.1.4.1.2021.8.1.101.1 UCD-SNMP-MIB::extOutput.1	Recuento de sesiones supervisadas abiertas
.1.3.6.1.4.1.2021.8.1.101.2 UCD-SNMP-MIB::extOutput.2	Solicitudes registradas por el proceso sniffer actual (establecido en cero para cada reinicio)
.1.3.6.1.4.1.2021.8.1.101.3 UCD-SNMP-MIB::extOutput.3	Indicación de fecha y hora de última sesión
.1.3.6.1.4.1.2021.8.1.101.4 UCD-SNMP-MIB::extOutput.4	Indicación de fecha y hora de última construcción
.1.3.6.1.4.1.2021.8.1.101.5 UCD-SNMP-MIB::extOutput.5	Memoria utilizada por el proceso sniffer
.1.3.6.1.4.1.2021.8.1.101.7 UCD-SNMP-MIB::extOutput.7	Paquetes de entrada en ETH1/ de salida en ETH2; normalmente sólo un número (entrada) cuando se utiliza un puerto SPAN o TAP
.1.3.6.1.4.1.2021.8.1.101.8 UCD-SNMP-MIB::extOutput.8	Paquetes de entrada en ETH3/ de salida en ETH4; normalmente sólo un número (entrada) cuando se utiliza un puerto SPAN o TAP
.1.3.6.1.4.1.2021.8.1.101.9 UCD-SNMP-MIB::extOutput.9	Paquetes de entrada en ETH5/ de salida en ETH6; normalmente sólo un número (entrada) cuando se utiliza un puerto SPAN o TAP

Otros MIB accesibles en la máquina son: SNMPv2-MIB, IF-MIB, RFC1213-MIB y HOST-RESOURCES-MIB.

Tema principal: Autosupervisión

Supervisor de consultas en ejecución

El Supervisor de consultas en ejecución muestra el estado de las consultas de usuario activas, y le permite establecer un valor de tiempo de espera para todas las consultas de informe/supervisor.

Abra Supervisor de consultas en ejecución pulsando Gestionar > Supervisión de actividad > Supervisor de consultas en ejecución.

En el Supervisor de consultas en ejecución, puede:

- Establecer el tiempo de espera de consulta para todos los informes y supervisores que se ejecutan en un portlet. Este valor de tiempo de espera no afecta a otros procesos de consulta, como simulaciones de política, procesos de auditoría o procesos internos. El valor predeterminado es 180 segundos (3 minutos).
- Interrumpa cualquier consulta de usuario que haya actualmente en ejecución. Algunas consultas que no se listan en este panel (por ejemplo, procesos de auditoría) pueden superar el tiempo de consulta especificado. Esto es lo que se espera, porque el valor de tiempo de espera de informe/supervisor se aplica sólo a los informes y supervisores en ejecución en un portlet.

No recomendamos establecer un tiempo de espera de consulta en un valor superior al valor predeterminado (180 segundos) durante mucho tiempo. Si establece este límite en un valor superior, se incrementa la probabilidad de sobrecargar el sistema con actividad de informes ad hoc.

Para cambiar el valor de tiempo de espera, especifique un número de segundos en el Tiempo de espera de informe/supervisor de consultas (segundos) y pulse Actualizar. Se le informará cuando finalice la actualización.

Tema principal: Autosupervisión

Grupos

La utilización de grupos facilita la creación y gestión de definiciones de clasificador, política y consulta, así como el despliegue de actualización en los clientes de GIM y S-TAP. En lugar de definir repetidamente un grupo de objetos de datos para una política de acceso, ponga los objetos en un grupo para gestionarlos fácilmente.

- Visión general de grupos
  Agrupe objetos de datos similares y utilícelos para crear definiciones de consulta, política y clasificación. Utilice uno de los muchos grupos predefinidos, o cree su propio grupo mediante el Creador de grupos.
- Utilización del creador de grupos
  El creador de grupos proporciona información global sobre la pertenencia a grupos y utiliza varias formas útiles para cumplimentarlos.
- Utilización del creador de grupos (antiguo)
- Utilización de grupos en consultas y políticas
  Breve visión general de los operadores condicionales para las consultas y dónde se utilizan los grupos en las políticas.
- Ejemplo: Utilización de grupos para crear reglas y políticas
  Utilice grupos para especificar rápidamente condiciones de regla en una política.
- Grupos predefinidos
  Esta sección detalla los grupos predefinidos de Guardium.

Tema principal: Gestión del sistema Guardium

Visión general de grupos

Agrupe objetos de datos similares y utilícelos para crear definiciones de consulta, política y clasificación. Utilice uno de los muchos grupos predefinidos, o cree su propio grupo mediante el Creador de grupos.

Hay muchos lugares donde los grupos son prácticos de utilizar. Agrupando objetos de datos similares, puede utilizar todo el conjunto de objetos en políticas, clasificaciones, consultas e informes, en lugar de tener que seleccionar individualmente varios objetos de datos.

Si necesita realizar cambios en una consulta o política, en lugar de aplicar estos cambios a cada objeto individual, puede aplicarlos al grupo.

Los S-TAP y GIM utilizan también grupos para facilitar el despliegue de actualizaciones en los servidores gestionados.

Creador de grupos

El Creador de grupos le permite crear un nuevo grupo o modificar un grupo existente desde la interfaz de usuario.

Abra el Creador de grupos pulsando Configuración > Creador de grupos.

La pantalla Filtro de grupos le permite ordenar fácilmente los grupos según el tipo de aplicación, el tipo de grupo, la descripción o la categoría.

Tipos de grupos

El campo Tipo de grupo hace referencia al tipo de datos que se agruparán. Por ejemplo, *IP de servidor* espera datos organizados como una dirección IP, y *Usuarios* espera ver los nombres de los usuarios en la aplicación.

Grupos de tuplas

Un grupo de tuplas permite que se combinen varios atributos para formar un único miembro de grupo compuesto. Un conjunto ordenado de tres valores se denomina una tupla de 3. Una tupla de n es un conjunto de n atributos de valor. Esto simplifica la especificación de las condiciones para los informes y las reglas de política.

Son ejemplos de grupos de tuplas:

- Grupos de tuplas: Objeto/Mandato, Objeto/Campo, IP de cliente/Usuario de BD, IP de servidor/Usuario de BD
- Grupos de tuplas de 3: IP de cliente/Programa de origen/Usuario de BD, Usuario de BD/Objeto/Privilegio

- Grupo de tuplas de 5: IP de cliente/Programa de origen/Usuario de BD/IP de servidor/Instancia de servicio
- Grupo de tuplas de 7: IP de cliente/Aplicación de origen/Usuario de BD/IP de servidor/Nombre de servicio/Usuario del SO/Nombre de BD

La tupla da soporte al uso de una barra inclinada y un carácter comodín (%). No da soporte al uso de una barra inclinada doble (//).
Nota: Consulta de tupla: Si el usuario intenta utilizar la condición LIKE GROUP y los datos contienen '\', es posible que el resultado no sea correcto. Si los datos contienen '\', el usuario debería utilizar en su lugar IN GROUP.

Grupos predefinidos

Existen varios grupos predefinidos incluidos con Guardium. Utilice el menú Filtro de grupos y Tipo de grupo para examinar la lista de grupos y encontrar el que se ajuste mejor a sus necesidades.

De forma predeterminada, los tipos de grupo *Usuario de BD/Contraseña de BD* sólo están disponibles para los usuarios de administración. Si desea cambiar este valor predeterminado, modifique los roles de grupo.

Solapamiento de pertenencias a grupos

Los miembros de grupo pueden estar en más de un grupo.

Por ejemplo, dos grupos predefinidos, *Crear mandatos* y *Mandatos DDL*, tienen ambos un miembro denominado CREATE TABLE. Si consulta cualquiera de estos dos grupos, se contabilizarán todos los miembros CREATE TABLE del periodo del informe en ese grupo.

En algunos casos, es posible que desee definir un conjunto de grupos de modo que cada miembro pertenezca a un único grupo. Por ejemplo, supongamos que para fines de informes necesita agrupar usuarios de base de datos en uno de estos dos grupos: empleados o asesores. Debería definir cada uno de estos grupos con el mismo tipo de subgrupo (por ejemplo, Empleado-Estado). Cuando se utilizan subgrupos, el sistema no le permitirá añadir un miembro a un subgrupo si este miembro ya se ha añadido a otro grupo con el mismo tipo de subgrupo.

Comodines en los miembros

Los miembros de grupo pueden incluir caracteres comodín (%) para cuando el grupo se utiliza en una condición de consulta o regla de política.

Tabla 1. Comodines en los miembros

Miembro	Coincide con	NO coincide con
aaa%	aaa aaazzz	zzzaaa aaz
%bbb	bbb,zzbbb	bb bbbzzz
%ccc%	ccc ccczz zzzccczzz	cc zzzcczzz

Grupos de unidades gestionadas

Existe una distinción entre grupos de unidades gestionadas y los grupos creados a través del creador de grupos utilizados para agrupar elementos para simplificar la creación y gestión de políticas y para clarificar la presentación de los informes. Para obtener más información sobre los grupos de unidades gestionadas, consulte Creación de grupos de unidades gestionadas.

Tema principal: Grupos

Utilización del creador de grupos

El creador de grupos proporciona información global sobre la pertenencia a grupos y utiliza varias formas útiles para cumplimentarlos.

Utilice el creador de grupos para crear y cumplimentar grupos desde distintos orígenes como, por ejemplo, archivos CSV, orígenes de datos externos o grupos existentes. Además, el constructor proporciona información global sobre la pertenencia a grupos, su utilización en políticas de seguridad, políticas de clasificación, consultas e informes.

Consejo:

Guardium V10.1.4 presenta una nueva interfaz de creación de grupos que se describe en esta información. Vaya a Configuración > Herramientas y vistas > Creador de grupos para acceder al nuevo creador de grupos.

El creador de grupos original es accesible en Configuración > Herramientas y vistas > Creador de grupos (Antiguo) y se describe en Utilización del creador de grupos (antiguo).

- Creación y edición de grupos
  Aprenda a crear y editar grupos.
- Visualización de la pertenencia a grupos y su utilización
  Aprenda a visualizar la pertenencia a grupos y a identificar políticas, informes y consultas en las que se utilizan los grupos.
- Cumplimentación de grupos
  El creador de grupos da soporte a varios métodos para añadir miembros a los grupos.

Tema principal: Grupos

Creación y edición de grupos

Aprenda a crear y editar grupos.

Tema principal: Utilización del creador de grupos

Creación de un grupo

Procedimiento

1. Abra el creador de grupos navegando a Configuración > Herramientas y vistas > Creador de grupos.
2. Pulse el icono en la tabla Creador de grupos.
3. Utilice el diálogo Crear nuevo grupo para definir un nuevo grupo. Proporcione una descripción de grupo y utilice los menús de Tipo de aplicación y de Tipo de grupo para definir el grupo.
4. Después de definir el nuevo grupo, utilice el separador Miembros para cumplimentar el grupo. Para obtener información sobre la cumplimentación de grupos, consulte Cumplimentación de grupos.
5. Pulse Guardar para acabar definiendo el nuevo grupo.

Edición de un grupo

Procedimiento

1. Abra el creador de grupos navegando a Configuración > Herramientas y vistas > Creador de grupos.
2. Seleccione un grupo de la tabla Creador de grupos y pulse el icono .
3. El recuadro Editar grupo sirve para modificar los valores del grupo. Para añadir más miembros al grupo o para modificar las pertenencias al grupo, utilice el separador Miembros. Para obtener información sobre la cumplimentación de grupos, consulte Cumplimentación de grupos.
4. Pulse Guardar para finalizar la edición del grupo.

Visualización de la pertenencia a grupos y su utilización

Aprenda a visualizar la pertenencia a grupos y a identificar políticas, informes y consultas en las que se utilizan los grupos.

Tema principal: Utilización del creador de grupos

Visualización de pertenencia a grupos

Acerca de esta tarea

Las columnas Miembros y Rellenado por de la tabla Creador de grupos resume el número de miembros en un grupo y cómo se cumplimenta. El siguiente procedimiento describe cómo se recupera la información detallada sobre la pertenencia al grupo y los métodos utilizados para cumplimentar el grupo.

Procedimiento

1. Abra el creador de grupos navegando a Configuración > Herramientas y vistas > Creador de grupos.
2. Abra el diálogo Editar grupo seleccionando un grupo de la tabla Creador de grupos y pulse el icono .
3. Visualice la pertenencia de grupo en el diálogo Editar grupo pulsando el separador Miembros.

Identificación de la utilización un grupo

Acerca de esta tarea

Las columnas Se utiliza en clasificador, Se utiliza en política y Se utiliza en consulta de la tabla Creador de grupos proporcionan una visión general de la utilización de los grupos en Guardium. El siguiente procedimiento describe cómo recuperar información detallada sobre las políticas, consultas e informes donde se utiliza un grupo.

Procedimiento

1. Abra el creador de grupos navegando a Configuración > Herramientas y vistas > Creador de grupos.
2. Abra el panel de detalles seleccionando un grupo de la tabla Creador de grupos y pulse Acciones > Ver detalles.
3. Utilice los separadores Políticas y Consultas en el panel detalles para ver dónde se utilizan los grupos seleccionados en políticas de seguridad, políticas de clasificador, consultas e informes.

Cumplimentación de grupos

El creador de grupos da soporte a varios métodos para añadir miembros a los grupos.

Procedimiento

1. Pulse el icono para crear un nuevo grupo o seleccionar un grupo de la tabla Creador de grupos y, a continuación, pulse el icono para editar un grupo existente.
2. Seleccione el separador Miembros del diálogo Crear nuevo grupo o Editar grupo.
3. Cumplimente el grupo utilizando uno de los siguientes métodos:
   - Utilice el icono para definir miembros de grupo de forma manual.
   - Utilice el menú Importar para añadir miembros de grupo utilizando uno de los siguientes métodos:
     - Desde CSV
     - Desde grupo
     - Desde origen de datos externo
     - Desde consulta

        - Desde LDAP

      Consejo: Una vez configurado, las acciones de importación que se puedan planificar aparecerán como separadores en el diálogo Crear nuevo grupo o Editar grupo. Acciones puntuales como, por ejemplo, Importar desde CSV no se pueden planificar y no añadirán un nuevo separador en el diálogo.
    - Algunos tipos de grupo también dan soporte a métodos avanzados para cumplimentar grupos, incluidos los siguientes:
        - Utilizando análisis de procedimiento almacenado en orígenes de datos
        - Utilizando dependencias de base de datos
        - Utilizando dependencias inversas
        - Utilizando procedimientos observados
        - Generando objetos seleccionados

      Importante: Al utilizar el creador de grupos añadido con Guardium V10.1.4, algunas acciones de importación avanzadas son invocadas en un grupo de destino que se cumplimenta en base a los resultados de un análisis realizado en un grupo de entrada seleccionado por el usuario. Esto representa un cambio en el comportamiento respecto al creador de grupos antiguo, donde las acciones avanzadas eran invocadas en un grupo de origen que contenía la entrada para ser analizada, importando los resultados del análisis en una grupo seleccionado por el usuario.

- Importación desde orígenes de datos externos
  Obtenga información sobre cómo puede completar rápidamente grupos de Guardium con datos de sus propias bases de datos y mantener estos grupos sincronizados con sus datos.

Tema principal: Utilización del creador de grupos

Importación desde orígenes de datos externos

Obtenga información sobre cómo puede completar rápidamente grupos de Guardium con datos de sus propias bases de datos y mantener estos grupos sincronizados con sus datos.

Acerca de esta tarea

Importar > Desde origen de datos externo automatiza la creación de tablas personalizadas, dominios y consultas para cumplimentar los grupos de Guardium desde sus propios orígenes de datos. Una vez que se han creado, estos artefactos representan una conexión duradera entre Guardium y sus datos: las actualizaciones de los datos se reflejan en los grupos de Guardium asociados.

Procedimiento

1. Seleccione Importar > Desde origen de datos externo para abrir el diálogo Importar desde origen de datos externo.
2. Utilice el menú Origen de datos para importar los datos desde un origen de datos. Pulse el icono para definir un nuevo origen de datos o el icono para editar un origen de datos existente.
3. Utilice los campos Nombre de tabla y Nombre de columna para identificar la ubicación de los datos que se importarán desde el origen de datos.
4. Pulse Aceptar para continuar.

Resultados

Si se completa el recuadro de diálogo Importar desde origen de datos externo, se crean o actualizan automáticamente los siguientes artefactos de Guardium:

- Tabla personalizada
- Origen de datos personalizado
- Dominio personalizado
- Consulta personalizada
- Grupo

Estos artefactos están disponibles a través de las herramientas de Guardium utilizando los convenios de denominación descritos en la siguiente tabla, donde *[nombre tabla]* y *[nombre columna]* se toman de los campos Nombre de tabla y Nombre de columna del diálogo Importar desde origen de datos externo.

Tabla 1. Importar desde origen de datos externo: resumen de artefactos creados.

Artefacto	Herramienta de Guardium	Convenio de denominación	Ejemplo	Planificado
Tabla personalizada	Creador de tablas personalizadas > Editar datos	*[nombre de tabla]_[nombre de columna]_[ID de origen de datos]*	`USERS_ADMIN_12345`	
Origen de datos personalizado	Creador de tablas personalizada > Subir datos	*[nombre de origen de datos]_[tipo de origen de datos](dominio personalizado)*	`user_repository(dominio personalizado)`	
Dominio personalizado	Creador de dominios personalizados	*[tipo de grupo]_[nombre de tabla]_[nombre de columna]_[ID de origen de datos]*	`USERS_USERS_ADMIN_12345`	
Consulta personalizada	Creador de consultas personalizadas	*[tipo de grupo]_[nombre de tabla]_[nombre de columna]_[ID de origen de datos]*	`USERS_USERS_ADMIN_12345`	
Grupo	Creador de grupos > Cumplimentar desde consulta		Usuarios administrativos de PCI	

Atención: Los nombres importados se truncan después de los 64 caracteres.
Tema principal: Cumplimentación de grupos

Utilización del creador de grupos (antiguo)

- Creación de un nuevo grupo
  Utilice el creador de grupos para crear de forma manual un grupo de objetos de datos.
- Modificación de un grupo
  Realice modificaciones en el grupo, como por ejemplo añadir un miembro o cambiar la categoría del grupo. Debe tener cuidado al modificar o suprimir un grupo, ya que los cambios realizados posiblemente podrían afectar a otros usuarios o políticas.

- Cumplimentación de grupos
  Tras crear un grupo o encontrar uno con el que desee trabajar, llene el grupo con miembros. Utilice el Creador de grupos (Antiguo) para añadir manualmente miembros a un grupo, o mediante diversos métodos de importación automatizados.

Tema principal: Grupos

Creación de un nuevo grupo

Utilice el creador de grupos para crear de forma manual un grupo de objetos de datos.

Procedimiento

1. Abra Creador de grupos pulsando Configuración > Creador de grupos (Antiguo).
2. Pulse Siguiente para omitir el filtro y crear un nuevo grupo.
3. En el panel Crear nuevo grupo, seleccione una opción en el menú Tipo de aplicación para determinar con qué aplicación utilizará el grupo.
4. Especifique una Descripción de grupo exclusiva para el nuevo grupo. No incluya apóstrofos en este campo.
5. Seleccione una Descripción de tipo de grupo para elegir el tipo de datos que está agrupando.
6. Especifique una Categoría, que es una etiqueta opcional que puede filtrar y utilizar para agrupar elementos (que el filtro ha aislado) de informes e infracciones de política.
7. Especifique una Clasificación, que es otra etiqueta opcional por la que puede filtrar y utilizar para agrupar elementos para informes e infracciones de política.
8. Seleccione Jerárquico para crear un grupo de grupos, donde el usuario de administración tenga acceso y, a continuación, páselo a los usuarios de los grupos de la jerarquía.
9. Pulse Añadir para añadir el grupo.

Tema principal: Utilización del creador de grupos (antiguo)

Modificación de un grupo

Realice modificaciones en el grupo, como por ejemplo añadir un miembro o cambiar la categoría del grupo. Debe tener cuidado al modificar o suprimir un grupo, ya que los cambios realizados posiblemente podrían afectar a otros usuarios o políticas.

Procedimiento

1. Abra Creador de grupos (Antiguo) pulsando Configuración > Creador de grupos (Antiguo).
2. Utilice el Filtro de grupo para encontrar el grupo que desea modificar, o deje el filtro vacío y pulse Siguiente para ver la lista completa de grupos.
3. Cuando modifique un grupo, una práctica recomendada es clonar el grupo , guardarlo como un nuevo grupo y, a continuación, modificar el clon para evitar efectos no deseados en el resto del sistema Guardium.

   El panel Modificar grupos existentes le permite:

   - Modificar, clonar o suprimir cualquier grupo
   - Asignar o modificar roles
   - Llenar el grupo a partir de una consulta, un servidor LDAP, o utilizando la funcionalidad Proxy de llamada generado automáticamente.
4. Con cualquier grupo seleccionado, pulse Modificar para poder:
   - modificar la categoría del grupo
   - añadir un miembro nuevo al grupo
   - renombrar un miembro de grupo
   - restablecer la pertenencia de un grupo a los miembros predefinidos
   - añadir comentarios
   - crear un alias para un grupo
   - rellenar un grupo desde LDAP

Tema principal: Utilización del creador de grupos (antiguo)

Modificación de la categoría de grupo

Procedimiento

Seleccione un grupo en la lista Miembros de grupo, especifique el nuevo nombre de categoría en el campo Categoría y pulse Modificar categoría para guardar los cambios.

Adición de un miembro de grupo

Cree un miembro nuevo y añádalo a un grupo, o añada un miembro existente a un grupo.

Procedimiento

Si tiene un miembro nuevo que desea añadir a un grupo, especifique el nombre del miembro en el campo Crear y añadir un nuevo miembro denominado y pulse Añadir.
Nota: Cuando se añade a un grupo de objetos, los nombres de miembros válidos se pueden componer de nombre_objeto, esquema.nombre_objeto, utilice un comodín como por ejemplo %nombre_objeto, o una combinación de los tres.
El miembro nuevo se ha añadido a la lista Miembros de grupo.

Cambio de nombre de un miembro de grupo

Procedimiento

1. Seleccione el miembro de grupo que se va a renombrar en la lista Miembros de grupo. Esto también mostrará el nombre del miembro de grupo actual en Renombrar miembro seleccionado como.
2. Cambie el nombre del miembro de grupo en el campo Renombrar miembro seleccionado como y pulse Actualizar.

Restablecimiento a la pertenencia a grupo predefinida

Pulse Restablecer en predefinido para cualquier grupo para sustituir los miembros actuales del grupo por el conjunto de miembros de grupo predefinidos.

Adición de un comentario a un grupo

Pulse Añadir comentarios para cualquier grupo para añadir comentarios para referencia futura.

Creación de un alias para un grupo

Procedimiento

1. Pulse Alias para abrir la ventana Definición rápida de alias.
2. Para cada miembro de grupo para el que desee crear un alias, especifique un valor en la columna Alias y pulse Aplicar.

Cumplimentación de grupos

Tras crear un grupo o encontrar uno con el que desee trabajar, llene el grupo con miembros. Utilice el Creador de grupos (Antiguo) para añadir manualmente miembros a un grupo, o mediante diversos métodos de importación automatizados.

- Cómo llenar un grupo desde LDAP
  Cómo importar datos desde un servidor LDAP para su uso en grupos de Guardium.
- Llenado de un grupo a partir de una consulta
  Cree una consulta y utilice los resultados para llenar un grupo. Esta opción de llenado de grupos es muy útil después de que la correlación de datos externa haya subido una tabla personalizada al sistema Guardium.
- Llenado de un grupo a partir de procedimientos almacenados
  Existen varios métodos para llenar grupos de mandatos o de objetos a partir de procedimientos almacenados. La funcionalidad Proxy de llamada generado automáticamente en el Creador de grupos le permite analizar grupos de mandatos o de objetos para miembros de grupo específicos y añadir esos miembros a un grupo nuevo.

Tema principal: Utilización del creador de grupos (antiguo)
Información relacionada:
Grupos y políticas de Guardium (vídeo)

Cómo llenar un grupo desde LDAP

Cómo importar datos desde un servidor LDAP para su uso en grupos de Guardium.

Acerca de esta tarea

Configure Guardium con el servidor LDAP y, a continuación, importe a petición o planifique una importación en el futuro.

Cuando se importan usuarios de LDAP:

- La cuenta de usuario de administración de Guardium no cambiará de ninguna forma.
- Tiene la opción de borrar los miembros existentes de un grupo antes de la importación.
- Las contraseñas de usuario existentes no cambiarán.
- De forma predeterminada, los usuarios nuevos están inhabilitados cuando se añaden, tienen asignado el rol user y tienen contraseñas en blanco.

Nota:

Los nombres de usuario no permiten caracteres especiales.

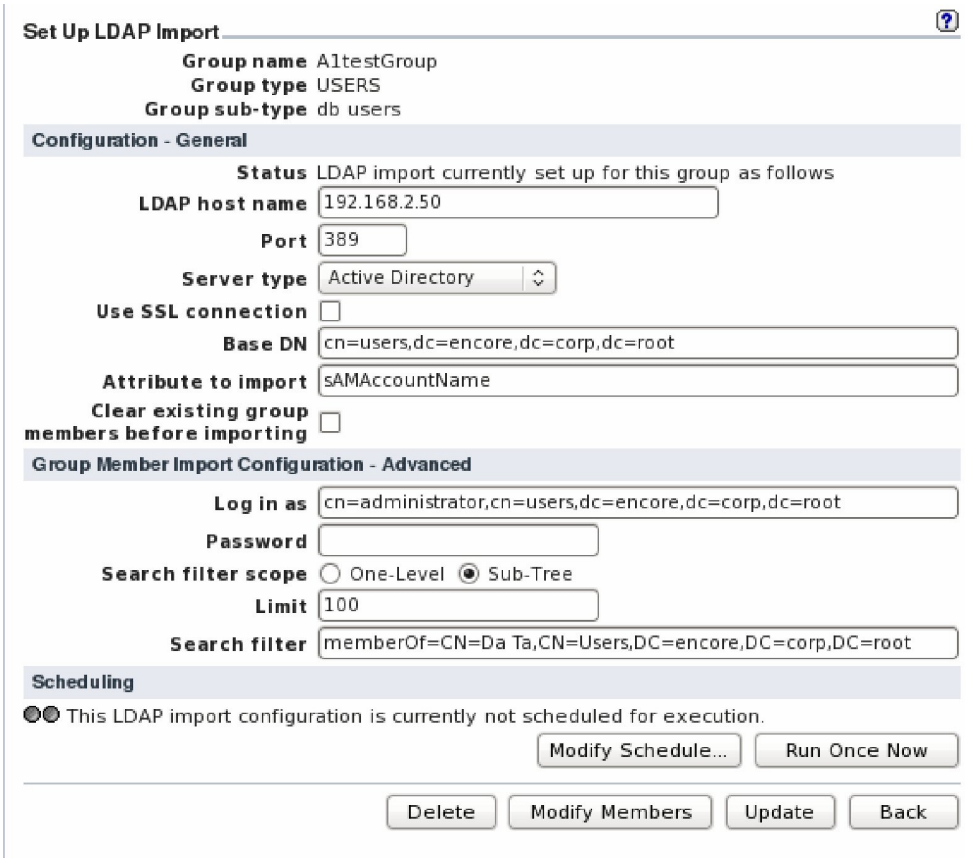
Si está planificando una importación, considere cualquier otra importación planificada que tenga en ese momento, ya que esto afectará al comportamiento de las importaciones planificadas existentes.

Procedimiento

Configure el servidor LDAP con el sistema Guardium. Abra el Creador de grupos pulsando Configuración > Creador de grupos (Antiguo) y cumplimente la información necesaria.

a. Para Nombre de host LDAP, especifique la dirección IP o nombre de host del servidor LDAP al que se accederá.
b. Para Puerto, especifique el número de puerto para conectar al servidor LDAP.
c. Seleccione el tipo de servidor LDAP del menú Tipo de servidor.
d. Marque el recuadro de selección Utilizar conexión SSL si Guardium se va a conectar al servidor LDAP utilizando una conexión SSL (Secure Socket Layer).
e. Para DN base, especifique el nodo en el árbol en el que desea empezar la búsqueda. Por ejemplo, un árbol de empresa podría empezar así: DC=encore,DC=corp,DC=root
f. Para Atributo a importar, especifique el atributo que se utilizará para importar usuarios (por ejemplo: cn). Cada atributo tiene un nombre y pertenece a una objectClass.
g. Marque el recuadro de selección Borrar miembros de grupo existentes antes de importar si desea suprimir todos los miembros de grupo existentes antes de importar.
h. Para Iniciar sesión como y Contraseña, especifique la información de cuenta de usuario que conectará al servidor de Guardium.
i. Para Ámbito de filtro de búsqueda, seleccione Un nivel para aplicar la búsqueda sólo al nivel base, o seleccione Subárbol para aplicar la búsqueda a los niveles situados debajo del nivel base.
j. Para Límite, especifique el número máximo de elementos que se devolverán. Le recomendamos que utilice este campo para probar nuevas consultas o modificaciones en las consultas existentes, de modo que no cargue un número excesivo de miembros.
k. Opcional: Para Filtro de búsqueda, defina un DN base, un ámbito y un filtro de búsqueda. Normalmente, las importaciones se basarán en la pertenencia a un grupo LDAP, de modo que se utilizaría la palabra clave memberOF. Por ejemplo: memberOf=CN=syyTestGroup,DC=encore,DC=corp,DC=root
l. Pulse Aplicar para guardar los valores de configuración.

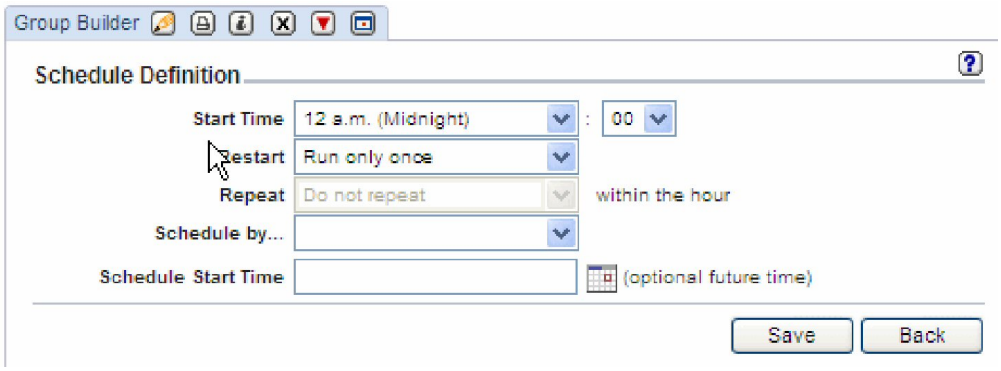
El indicador Estado de la sección Configurado-General cambiará a *Actualmente la importación de LDAP está configurada para este grupo tal como sigue* y se habilitarán los botones Modificar planificación y Ejecutar una vez ahora. Ahora puede importar desde el servidor LDAP.



Qué hacer a continuación

Ejecute o planifique un informe.

- Planifique una importación de LDAP pulsando Modificar planificación, rellenando la información de planificación y a continuación pulsando Guardar.



- Para ejecutar la importación a petición, pulse Ejecutar una vez ahora. Cuando se complete la tarea, el conjunto de miembros que cumplan los criterios de selección se mostrará en el panel Resultados de consulta LDAP.

Nota:

Cuando se importa a petición, tiene la oportunidad de aceptar o rechazar cada entrada devuelta del servidor LDAP.

Cuando se planifica una importación de LDAP, se importarán todas las entradas LDAP que coincidan con los criterios de búsqueda.

Verifique que los miembros se hayan añadido a un grupo seleccionando el grupo en el Creador de grupos y pulsando a continuación Modificar y comprobando la pertenencia del grupo.

Para grupos más grandes, puede resultar más fácil verificar los miembros mediante el informe Detalles del grupo de Guardium (Informes > Detalles del grupo de Guardium).

Tema principal: Cumplimentación de grupos

Llenado de un grupo a partir de una consulta

Cree una consulta y utilice los resultados para llenar un grupo. Esta opción de llenado de grupos es muy útil después de que la correlación de datos externa haya subido una tabla personalizada al sistema Guardium.

Procedimiento

1. Abra Creador de grupos pulsando Configuración > Creador de grupos (Antiguo).Utilice el filtro para encontrar el grupo que desea llenar, o pulse Siguiente y busque el grupo en la lista de todos los grupos.
2. Con un grupo seleccionado, pulse el botón Cumplimentar desde consulta para abrir el panel Cumplimentar grupo desde configuración de consulta.
3. En el menú Consulta, seleccione la consulta que se va a ejecutar.
    a. En función del tipo de grupo que se esté llenando, aparecerán diferentes campos. Para la mayoría de los tipos de grupo, aparecerá el menú Miembro de captación desde columna.
    b. Para los grupos de atributos emparejados (Objeto/Mandato, Objeto/Campo o IP de cliente/Usuario de BD), aparecerán dos menús: Elegir columna para el atributo 1 y Elegir columna para el atributo 2.
    c. Seleccione la columna (o columnas) que se utilizarán para llenar el grupo y los parámetros adicionales para la consulta. A continuación, los parámetros de tiempo de ejecución de la consulta se añadirán al panel.
4. Marque el recuadro de selección Borrar miembros de grupo existentes antes de importar si desea suprimir todo el contenido del grupo existente antes de importar miembros nuevos.
5. Opcional: Seleccione un origen remoto (sólo disponible desde un Gestor central).
6. Pulse Guardar para guardar la definición.
7. Pulse Ejecutar una vez ahora para ejecutar la consulta inmediatamente o bien pulse Modificar planificación para establecer una planificación para la consulta en el futuro.

Tema principal: Cumplimentación de grupos

Llenado de un grupo a partir de procedimientos almacenados

Existen varios métodos para llenar grupos de mandatos o de objetos a partir de procedimientos almacenados. La funcionalidad Proxy de llamada generado automáticamente en el Creador de grupos le permite analizar grupos de mandatos o de objetos para miembros de grupo específicos y añadir esos miembros a un grupo nuevo.

Acerca de esta tarea

El Creador de grupos (Antiguo) puede llenar automáticamente los tipos de grupo de mandato o de objetos de dos formas:

- Analizando el código fuente del procedimiento almacenado. Para utilizar esta opción, Guardium debe acceder a la base de datos en la que se han definido los procedimientos almacenados, y los procedimientos almacenados no se deben almacenar en formato cifrado.
- Analizando los procedimientos almacenados en el tráfico de base de datos que Guardium ha supervisado y registrado. Para utilizar esta opción, el dispositivo de Guardium debe estar inspeccionando las corrientes de datos de base de datos apropiadas y registrando la información (en lugar de utilizar las acciones de omitir sesión u omitir registro), y la tarea de análisis se debe ejecutar mientras los datos aún están en la unidad (en lugar de, por ejemplo, después de una operación de archivado/depuración).

Hay dos grupos implicados al llenar un grupo a partir de procedimientos almacenados:

- El grupo receptor es el grupo al que se añadirán los miembros.
- El grupo inicial que se analizará. Este grupo debe ser un grupo de objetos o mandatos existente. El proceso de búsqueda y adición es recursivo. Por ejemplo, si el procedimiento almacenado denominado prox_one se añade al grupo receptor, y prox_one se referencia en prox_two, prox_two también se añadirá al grupo receptor.

Nota: Los comodines no están soportados en el campo de miembros de grupo para procedimientos almacenados.

Procedimiento

1. Abra Creador de grupos pulsando Configuración > Creador de grupos (Antiguo).
2. Elija un grupo inicial para analizar que sea un grupo de tipo de mandatos o de objetos.
3. Con el grupo inicial seleccionado, pulse Proxy de llamada generado automáticamente. Se le presentarán cinco opciones:
    a. Utilizando orígenes de BD: Llene un grupo analizando las definiciones de procedimiento almacenado de una o varias bases de datos.
    b. Utilizando dependencias de base de datos: Llene un grupo de objetos o un grupo de objetos calificados mediante el análisis de funciones, clases Java, paquetes, procedimientos, sinónimos, tablas, desencadenantes y/o vistas.
    c. Utilizando dependencias inversas: Llene un grupo calculando un conjunto de objetos utilizados al iniciar desde un conjunto de objetos.
    Nota: La opción Utilizando dependencias inversas sólo está disponible para Oracle.
    d. Utilizando procedimientos observados: Llene un grupo mediante el análisis de los mandatos CREATE PROCEDURE y ALTER PROCEDURE tal como se observa en el tráfico de la base de datos.
    e. Generar objeto seleccionado: Llene un grupo mediante el análisis inverso de los procedimientos almacenados. Empezando por un conjunto de procedimientos almacenados, calcule todas las tablas que utilizan estos procedimientos (directa o indirectamente).
    Nota: La opción Generar objeto seleccionado sólo se puede utilizar con tipo de grupo de objetos.

- Llenado de un grupo utilizando orígenes de base de datos
- Llenado de un grupo utilizando dependencias de base de datos
  Utilice esta opción para llenar grupos según las dependencias de base de datos como, por ejemplo, funciones, clases Java, paquetes, procedimientos, sinónimos, tablas, desencadenantes y/o vistas. **Esta opción sólo funcionará con bases de datos de Oracle en tipos de grupos de objetos.** Esta opción no funciona en tipos de grupo de *mandatos* porque la información de dependencia en la base de datos sólo está relacionada con objetos.
- Llenado de un grupo utilizando dependencias inversas
  Generar objeto seleccionado llena el grupo mediante el análisis inverso de los procedimientos almacenados observados.
- Llenado de un grupo utilizando procedimientos observados
  Guardium llenará un grupo inspeccionando todos los cambios o adiciones a los procedimientos almacenados. Esto mantiene la información de correlación actualizada mediante el análisis continuo de los cambios en los procedimientos almacenados.
- Llenado de un grupo utilizando Generar objeto seleccionado
  La opción Generar objeto seleccionado es una parte de la funcionalidad Proxy de llamada generado automáticamente que llena un tipo de grupo de objetos mediante el análisis inverso de los procedimientos almacenados observados.

Tema principal: Cumplimentación de grupos

Llenado de un grupo utilizando orígenes de base de datos

Antes de empezar

Para utilizar esta opción:

- Debe saber dónde están definidos los procedimientos almacenados que le interesan.
- Los orígenes no deben almacenarse en formato cifrado.
- Debe tener acceso a los orígenes de los procedimientos almacenados en estas bases de datos.

Acerca de esta tarea

Guardium analizará el código fuente del procedimiento almacenado en uno o más servidores de bases de datos. Seleccione un grupo y, a continuación, ejecute el proceso Proxy de llamada generado automáticamente para explorar los procedimientos almacenados. Este proceso comprobará el grupo seleccionado para ver si se puede acceder a alguno de los objetos de ese grupo o si se puede ejecutar alguno de los mandatos de ese grupo. Las coincidencias se añadirán a un grupo nuevo. Para llenar un grupo utilizando orígenes de base de datos:

Procedimiento

1. Abra Creador de grupos pulsando Configuración > Creador de grupos (Antiguo).Utilice el filtro para encontrar el grupo que desea llenar, o pulse Siguiente y busque el grupo en la lista de todos los grupos.
   Nota: Esta opción sólo se puede utilizar con tipos de grupo de objetos o mandatos.
2. Con el grupo seleccionado, pulse Proxy de llamada generado automáticamente y seleccione la opción Utilizando orígenes de BD. Se abrirá el panel Analizar procedimientos almacenados.
3. Pulse Añadir origen de datos y seleccione un origen de datos en el Buscador de orígenes de datos. El origen de datos seleccionado aparecerá en el panel Orígenes de datos.
4. Opcional: Rellene los Parámetros de consulta. Algunos campos sólo se aplican a determinadas bases de datos.
   - **Para Sybase, MS SQL Server e Informix**, especifique un nombre de base de datos para restringir la operación a dicha base de datos. Si está en blanco, se analizarán todos los procedimientos almacenados de la base de datos maestra.
   - **Sólo para MySQL, Oracle o DB2**, especifique un nombre de esquema para restringir la operación a las bases de datos que son propiedad de ese esquema. Sólo para MySQL, el propietario de esquema tiene el formato nombre_usuario@host, donde host puede ser una IP específica o puede ser un % para especificar todos los hosts. Para obtener todos los hosts, especifique el nombre de esquema seguido de %.
   - **Sólo para MySQL, Oracle o DB2**, especifique un nombre de procedimiento almacenado en Nombre de objeto. Pueden utilizarse caracteres comodín. Por ejemplo, si sólo está interesado en los procedimientos que empiezan por las letras ABC, escriba ABC% en el recuadro Nombre de objeto.
5. En la sección Configuración de detalle de origen, realice una de las acciones siguientes:
   - Añada miembros a un grupo existente marcando el recuadro de selección Añadir y, a continuación, seleccionando un grupo en el menú Nombre de grupo existente.
   - Añada miembros a un grupo nuevo especificando el nuevo nombre de grupo en Nombre de nuevo grupo.
     Nota: No incluya apóstrofos en un nombre de grupo.
6. Seleccione Espacio de nombres de uniformado para crear nombres de miembro utilizando caracteres comodín, de modo que el grupo pueda utilizarse para comparaciones LIKE GROUP. Por ejemplo, si se descubre sp_1, el miembro %sp_1% se añadirá al grupo y, en una comparación LIKE GROUP, coincidirían todos los valores sp_101, sp_102, sss_sp_103, etc.
7. Pulse Analizar base de datos para empezar a llenar el grupo. La operación puede tardar mucho tiempo en completarse.

Tema principal: Llenado de un grupo a partir de procedimientos almacenados

Llenado de un grupo utilizando dependencias de base de datos

Utilice esta opción para llenar grupos según las dependencias de base de datos como, por ejemplo, funciones, clases Java, paquetes, procedimientos, sinónimos, tablas, desencadenantes y/o vistas. **Esta opción sólo funcionará con bases de datos de Oracle en tipos de grupos de objetos.** Esta opción no funciona en tipos de grupo de *mandatos* porque la información de dependencia en la base de datos sólo está relacionada con objetos.

Acerca de esta tarea

Cuando especifique el tipo de grupo, tenga en cuenta que sólo los tipos de grupo de *objetos* u *objetos cualificados* funcionan con esta opción. Un objeto cualificado requiere cinco atributos de valor: IP de servidor, instancia, nombre de BD, propietario y objeto. Esto también se denomina objeto de tuplas de 5.

Un ejemplo de cómo es un miembro de grupo de objetos cualificados es un objeto 192.168.1.0+custum+oracle+admin+fininacial.

Procedimiento

1. Abra Creador de grupos pulsando Configuración > Creador de grupos (Antiguo).Utilice el filtro para encontrar el grupo que desea llenar, o pulse Siguiente y busque el grupo en la lista de todos los grupos.
2. Con el grupo de objetos o de objetos cualificados seleccionado, pulse Proxy de llamada generado automáticamente y seleccione la opción Utilizando dependencias de base de datos. Se abrirá el panel Analizar procedimientos almacenados.
3. Pulse Añadir origen de datos y seleccione un origen de datos en el Buscador de orígenes de datos. El origen de datos seleccionado aparecerá en el panel Orígenes de datos.
4. Opcional: Rellene los Parámetros de consulta.
5. En la sección Configuración de detalle de origen, realice una de las acciones siguientes:
   - Añada miembros a un grupo existente marcando el recuadro Añadir y, a continuación, seleccionando un grupo en el menú Nombre de grupo existente.
   - Añada miembros a un grupo nuevo especificando el nuevo nombre de grupo en Nombre de nuevo grupo.
     Nota: No incluya apóstrofos en un nombre de grupo, y asegúrese de que el nuevo grupo esté totalmente calificado (incluya cinco atributos de valor: IP de servidor, instancia, nombre de BD, propietario y objeto).
6. Seleccione Espacio de nombres de uniformado para crear nombres de miembro utilizando caracteres comodín, de modo que el grupo pueda utilizarse para comparaciones LIKE GROUP. Por ejemplo, si se descubre sp_1, el miembro %sp_1% se añadirá al grupo y, en una comparación LIKE GROUP, coincidirían todos los valores sp_101, sp_102, sss_sp_103, etc.

7. En la sección Tipos de inclusión, seleccione dependencias de base de datos: funciones, clases Java, paquetes, procedimientos, sinónimos, tablas, desencadenantes y/o vistas.
8. Pulse Analizar base de datos para llenar el grupo. Se le informará de los resultados.

Tema principal: Llenado de un grupo a partir de procedimientos almacenados

Llenado de un grupo utilizando dependencias inversas

Generar objeto seleccionado llena el grupo mediante el análisis inverso de los procedimientos almacenados observados.

Acerca de esta tarea

Estas opciones del menú de llenado automático de grupo calculan conjunto de objetos utilizados al iniciar desde un conjunto de objetos. Por ejemplo, a partir de un conjunto de procedimientos almacenados, calcule todas las tablas que utilizan estos procedimientos (directa o indirectamente).

Procedimiento

1. Abra Creador de grupos pulsando Configuración > Creador de grupos (Antiguo).Utilice el filtro para encontrar el grupo que desea llenar, o pulse Siguiente y busque el grupo en la lista de todos los grupos.
   Nota: La opción Dependencias inversas sólo está disponible para Oracle.
2. Con el grupo seleccionado, pulse Proxy de llamada generado automáticamente y seleccione la opción Utilizando dependencias inversas. Se abrirá el panel Analizar procedimientos almacenados.
3. Pulse Añadir origen de datos y seleccione un origen de datos en el Buscador de orígenes de datos. El origen de datos seleccionado aparecerá en el panel Orígenes de datos.
4. Opcional: Rellene los Parámetros de consulta.
5. En la sección Configuración de detalle de origen, realice una de las acciones siguientes:
   - Para añadir miembros a un grupo existente, seleccione Añadir y, a continuación, seleccione el grupo en la lista Nombre de grupo existente.
   - Para añadir miembros a un grupo nuevo, especifique el nuevo nombre de grupo en Nombre de nuevo grupo.
     Nota: No incluya apóstrofos en un nombre de grupo.
6. Seleccione Espacio de nombres de uniformado para crear nombres de miembro utilizando caracteres comodín, de modo que el grupo pueda utilizarse para comparaciones LIKE GROUP. Por ejemplo, si se descubre sp_1, el miembro %sp_1% se añadirá al grupo y, en una comparación LIKE GROUP, coincidirían todos los valores sp_101, sp_102, sss_sp_103, etc.
7. En la sección Tipos de inclusión, seleccione dependencias de base de datos: funciones, clases Java, paquetes, procedimientos, sinónimos, tablas, desencadenantes y/o vistas.
8. Pulse Analizar base de datos para llenar el grupo. Se le informará de los resultados.

Tema principal: Llenado de un grupo a partir de procedimientos almacenados

Llenado de un grupo utilizando procedimientos observados

Guardium llenará un grupo inspeccionando todos los cambios o adiciones a los procedimientos almacenados. Esto mantiene la información de correlación actualizada mediante el análisis continuo de los cambios en los procedimientos almacenados.

Procedimiento

1. Abra Creador de grupos pulsando Configuración > Creador de grupos (Antiguo).Utilice el filtro para encontrar el grupo que desea llenar, o pulse Siguiente y busque el grupo en la lista de todos los grupos.
2. Con el grupo inicial seleccionado, pulse Proxy de llamada generado automáticamente y seleccione la opción Utilizando procedimientos observados. Se abrirá el panel Analizar procedimientos almacenados observados.
3. Para editar una configuración existente, selecciónela en el menú Detalles de origen. Para crear una nueva configuración, deje la selección en *Nuevo*.
4. En la sección Información de acceso, seleccione todos los servidores de bases de datos que se van a analizar. Puede elegir cualquier combinación de los recuadros de selección.
5. En la sección Configuración de detalle de origen, realice una de las acciones siguientes:
   - Añada miembros a un grupo existente marcando el recuadro Añadir y, a continuación, seleccionando un grupo en el menú Nombre de grupo existente.
   - Añada miembros a un grupo nuevo especificando el nuevo nombre de grupo en Nombre de nuevo grupo.
     Nota: No incluya apóstrofos en un nombre de grupo.
6. Seleccione Espacio de nombres de uniformado para crear nombres de miembro utilizando caracteres comodín, de modo que el grupo pueda utilizarse para comparaciones LIKE GROUP. Por ejemplo, si se descubre sp_1, el miembro %sp_1% se añadirá al grupo y, en una comparación LIKE GROUP, coincidirían todos los valores sp_101, sp_102, sss_sp_103, etc.
7. Pulse Guardar para guardar la configuración.
8. Establezca una planificación para el grupo realizando una de las acciones siguientes:
   - Para ejecutar la consulta inmediatamente y obtener resultados ahora, pulse Ejecutar una vez ahora.
   - Para definir una planificación para la operación, pulse Modificar planificación.

Tema principal: Llenado de un grupo a partir de procedimientos almacenados

Llenado de un grupo utilizando Generar objeto seleccionado

La opción Generar objeto seleccionado es una parte de la funcionalidad Proxy de llamada generado automáticamente que llena un tipo de grupo de objetos mediante el análisis inverso de los procedimientos almacenados observados.

Acerca de esta tarea

Guardium llenará el grupo inspeccionando todos los cambios o adiciones a los procedimientos almacenados. Esto mantiene la información de correlación actualizada mediante el análisis continuo de los cambios en los procedimientos almacenados.

Procedimiento

1. Abra Creador de grupos pulsando Configuración > Creador de grupos (Antiguo).Utilice el filtro para encontrar el grupo que desea llenar, o pulse Siguiente y busque el grupo en la lista de todos los grupos.
2. Con el grupo inicial seleccionado, pulse Proxy de llamada generado automáticamente y seleccione la opción Generar objeto seleccionado. Se abrirá el panel Analizar procedimientos almacenados observados.
3. Para editar una configuración existente, selecciónela en el menú Detalles de origen. Para crear una configuración nueva, pulse *Nueva*.
4. En la sección Información de acceso, seleccione todos los servidores de bases de datos que se van a analizar. Puede elegir cualquier combinación de los recuadros de selección.
5. En la sección Configuración de detalle de origen, especifique un nombre y elija una opción en el menú Verbo.
6. Realice una de las opciones siguientes:
   - Añada miembros a un grupo existente marcando el recuadro Añadir y, a continuación, seleccionando un grupo en el menú Nombre de grupo existente.
   - Añada miembros a un grupo nuevo especificando el nuevo nombre de grupo en Nombre de nuevo grupo.
     Nota: No incluya apóstrofos en un nombre de grupo.
7. Seleccione Espacio de nombres de uniformado para crear nombres de miembro utilizando caracteres comodín, de modo que el grupo pueda utilizarse para comparaciones LIKE GROUP. Por ejemplo, si se descubre sp_1, el miembro %sp_1% se añadirá al grupo y, en una comparación LIKE GROUP, coincidirían todos los valores sp_101, sp_102, sss_sp_103, etc.
8.
9. Pulse Guardar para guardar la configuración.
10. Establezca una planificación para el grupo realizando una de las acciones siguientes:
    - Para ejecutar la consulta inmediatamente y obtener resultados ahora, pulse Ejecutar una vez ahora.
    - Para definir una planificación para la operación, pulse Modificar planificación.

Tema principal: Llenado de un grupo a partir de procedimientos almacenados

Utilización de grupos en consultas y políticas

Breve visión general de los operadores condicionales para las consultas y dónde se utilizan los grupos en las políticas.

Consultas

Las consultas utilizan operadores condicionales con grupos. A continuación se muestran ejemplos de cada operador condicional:

- IN GROUP: Si el valor coincide con cualquier miembro del grupo seleccionado, la condición es true. IN ALIASES GROUP: Este operador funciona con un grupo del mismo tipo que IN GROUP, pero presupone que los miembros de ese grupo son alias. Tenga en cuenta que los operadores IN GROUP/IN ALIASES GROUP esperan que el grupo contenga valores reales o alias, respectivamente. El Creador de consultas buscará registros con valores de base de datos que coincidan con el valor de los alias del grupo.
- NOT IN GROUP: Si el valor no coincide con ningún miembro del grupo seleccionado, la condición es true. NOT IN ALIASES GROUP: Funciona con un grupo del mismo tipo que NOT IN GROUP, pero supone que los miembros de ese grupo son alias.
- IN DYNAMIC GROUP: Si el valor coincide con cualquier miembro de un grupo que nombrará como un parámetro de tiempo de ejecución, la condición es true. IN DYNAMIC ALIASES GROUP: Funciona con un grupo del mismo tipo que IN DYNAMIC GROUP, pero supone que los miembros de ese grupo son alias.
- NOT IN DYNAMIC GROUP: Si el valor no coincide con ningún miembro de un grupo que se vaya a nombrar como un parámetro de tiempo de ejecución, la condición es true. NOT IN DYNAMIC ALIASES GROUP: Funciona con un grupo del mismo tipo que NOT IN DYNAMIC GROUP, pero supone que los miembros de ese grupo son alias.
  Nota: El grupo puede contener alias o valores reales según el operador utilizado IN GROUP e IN ALIASES GROUP no se pueden utilizar al mismo tiempo.
- LIKE GROUP: Si el valor es similar a cualquier miembro del grupo seleccionado, la condición es verdadera. Esta condición permite comodines (%) en los nombres de miembro del grupo.
  Nota: Un valor like member utiliza uno o más comodines (%) y coincide con todo o parte del valor. Para una comparación like, los caracteres alfabéticos no son sensibles a las mayúsculas y minúsculas. Por ejemplo, %tea% coincidiría con tea, TeA, tEam o steam.

Políticas y reglas

Cuando se crea una regla como parte de una política, los grupos simplifican el proceso de especificación de los parámetros que desea.

puede seleccionar un grupo en cualquier lugar donde haya un menú desplegable Grupo en el panel de definición de regla.

Además, si desea crear o modificar un grupo sobre la marcha, pulse el icono Grupos para abrir una ventana Definición de grupo y realizar los cambios que desee.

Por ejemplo: si desea capturar actividad que se produce en los servidores de producción, en lugar de escribir cada vez direcciones IP completas, podría crear un grupo *Servidores de producción* y utilizarlo.

Tema principal: Grupos

Ejemplo: Utilización de grupos para crear reglas y políticas

Utilice grupos para especificar rápidamente condiciones de regla en una política.

Acerca de esta tarea

Cada política se compone de una o más reglas. Especifique qué condiciones ejecutarán una regla, y a continuación elija una o más acciones que se realizarán cuando se desencadene esa regla. Este ejemplo le muestra cómo utilizar grupos para identificar usuarios no autorizados, registrar detalles de su acceso en un grupo de objetos confidenciales y enviar una alerta que indique que se ha producido el acceso.

Procedimiento

1. Inicie sesión en el sistema Guardium y abra el Creador de políticas pulsando Configuración > Herramientas y vistas > Creador de políticas para datos.
2. Cree una nueva política pulsando el icono para abrir la ventana Definición de política.
3. Defina la definición de política y a continuación pulse Aplicar para guardar la política.
4. Pulse Editar reglas para abrir la ventana Reglas de política y empiece a añadir reglas a la política.
5. Pulse Añadir reglas > Añadir regla de acceso para añadir una nueva regla a la política.

6. Empiece proporcionando una Descripción para la regla. Opcionalmente, proporcione las etiquetas Categoría y Clasificación.
7. Especifique dónde se deben buscar los datos. En la fila IP de servidor, seleccione el grupo PCI - IP de servidores autorizados (públicos). La regla se aplicará a toda la actividad de todos los servidores PCI.
   Nota: Para ver los miembros de un grupo o modificar un grupo, vaya al Creador de grupos.
8. Especifique los usuarios no autorizados. En la fila Usuario de BD, marque el recuadro de selección No y seleccione el grupo Usuarios autorizados (públicos). La regla se aplicará a todos los usuarios que no están en el grupo *Usuarios autorizados (públicos)*.
9. Especifique los objetos confidenciales. En la fila Objeto, seleccione el grupo PCI - Objetos confidenciales de los titulares de tarjeta (públicos). La regla se aplicará ahora a todos los usuarios no autorizados en servidores PCI que busquen acceder a objetos confidenciales PCI.
10. Añada una acción a la regla pulsando Añadir acción y seleccionando Acción > REGISTRAR TODOS LOS DETALLES en el menú. Pulse Aplicar para guardar la regla. Esta acción registra los detalles del acceso, incluida la indicación de fecha y hora exacta del acceso.
11. Añada otra acción a la regla pulsando Añadir acción y seleccionando Acción > ALERTAR UNA VEZ POR SESIÓN en el menú. Especifique un destino de alerta y a continuación pulse Aplicar para guardar la regla. Esta acción envía o registra una alerta que indica que se ha desencadenado la regla.
12. Pulse Guardar para guardar la regla.
13. Instale la política.
    a. Busque la política que ha creado. Pulse Atrás dos veces, o pulse Creador de políticas para ir al Buscador de políticas y examinar la lista de políticas.
    b. Con la política seleccionada, elija Instalar y modificar en el menú de acciones de instalación.
    c. Pulse Aceptar para confirmar la instalación de la política y a continuación marque Últimos registros e infracciones para verificar que la política se ha instalado.

       La política está ahora instalada y activa. Se registrará la sesión de cualquier persona que no esté en el grupo *Usuarios autorizados (públicos)* que intente acceder a un objeto de los grupos *PCI - Objetos confidenciales de los titulares de tarjeta (públicos)* y se desencadenará una alerta que indicará el acceso.

Tema principal: Grupos

Grupos predefinidos

Esta sección detalla los grupos predefinidos de Guardium.

La tabla siguiente describe los grupos predefinidos incluidos con el sistema Guardium. Para ver la lista de todos los grupos, abra el Creador de grupos pulsando Configuración > Creador de grupos. Seleccione *SQL_APP_NAME* en el menú Aplicaciones y pulse Siguiente. En la pantalla siguiente, gestione los miembros de los grupos seleccionados. El término *Tipo de grupo* hace referencia a las expectativas sobre el tipo de datos designados por la etiqueta. Por ejemplo, el tipo de grupo *IP de servidor* espera datos organizados como una dirección IP (192.168.1.0) y el tipo de grupo *Usuarios* espera ver nombres de usuarios de la aplicación.

Periódicamente se añaden grupos predefinidos adicionales y es posible que estos grupos predefinidos no se describan aquí. Abra el Creador de grupos para ver todos los grupos existentes.

Se permiten grupos predefinidos de tipo de grupo Usuario de BD/Contraseña de BD sólo a los usuarios con el rol de admin. Los usuarios pueden, si se prefiere, añadir otros roles o incluso permitir los grupos a todos los roles.

Tabla 1. Grupos predefinidos

SQL_APP_NAME	GROUP_DESCRIPTION	MEMBERS
Grupos de zOS de DB2	SQL dinámico de auditoría zOS	Tipo de grupo para mandatos de DB2
Grupos de zOS de DB2	Consulta de auditoría de zOS	Tipo de grupo para mandatos de DB2
Grupos de zOS de DB2	Actualizaciones de auditoría de zOS	Tipo de grupo para mandatos de DB2
Grupos de zOS de DB2	Supresiones de auditoría de zOS	Tipo de grupo para mandatos de DB2
Grupos de zOS de DB2	Inserciones de auditoría de zOS	Tipo de grupo para mandatos de DB2
Grupos de zOS de DB2	Programas de utilidad de auditoría de zOS	Tipo de grupo para mandatos de DB2
Grupos de zOS de DB2	Mantenimiento de objetos de auditoría de zOS	Tipo de grupo para mandatos de DB2
Grupos de zOS de DB2	Mantenimiento de usuarios de auditoría de zOS	Tipo de grupo para mandatos de DB2
Grupos de zOS de DB2	Cambios de autorización de usuario de auditoría de zOS	Tipo de grupo para mandatos de DB2
Grupos de zOS de DB2	Mandatos DB2 de auditoría de zOS	Tipo de grupo para mandatos de DB2
Grupos de zOS de DB2	Mantenimiento de paquetes/planes de auditoría de zOS	Tipo de grupo para mandatos de DB2
Grupos de zOS de IMS	Consulta de auditoría de IMS de zOS	Tipo de grupo para mandatos de IMS
Grupos de zOS de IMS	Actualizaciones de auditoría de IMS de zOS	Tipo de grupo para mandatos de IMS
Grupos de zOS de IMS	Supresiones de auditoría de IMS de zOS	Tipo de grupo para mandatos de IMS
Grupos de zOS de IMS	Inserciones de auditoría de IMS de zOS	Tipo de grupo para mandatos de IMS
Grupos de zOS de IMS	Mandatos de BD de auditoría de IMS de zOS	Tipo de grupo para mandatos de IMS
Creador de políticas	Objetos del titular de la tarjeta	Tipo de grupo, objetos
Creador de políticas	Objetos financieros	Tipo de grupo, objetos
Creador de políticas	Objetos PHI	Tipo de grupo, objetos
Creador de políticas	IP de clientes autorizados	Tipo de grupo, IP de cliente
Creador de políticas	Usuarios de producción	Tipo de grupo, usuarios
Creador de políticas	Objetos PII	Tipo de grupo, objetos
Creador de políticas	Servidores de producción	Tipo de grupo, IP de servidor
Creador de políticas	Servidores financieros	Tipo de grupo, IP de servidor

SQL_APP_NAME	GROUP_DESCRIPTION	MEMBERS
Creador de políticas	Usuarios funcionales	Tipo de grupo, usuarios
Creador de políticas	Servidores Sharepoint	Tipo de grupo, IP de servidor
Creador de asesoramientos de seguridad	DB2 Database Version+Patches Informix Database Version+Patches MS Sql Server Database Version+Patches MySql Database Version+Patches Netezza Version+Patches Oracle Database Version+Patches Postgress Version+Patches Sybase Database Version+Patches Teradata PDE Version+Patches Teradata TDBMS Version+Patches Teradata TDGSS Version+Patches Teradata TGTW Version+Patches	Se utiliza para pruebas de nivel de parche y versión de base de datos (específicas).
Creador de asesoramientos de seguridad	DB2 Allowed Grants to Public Informix Allowed Grants to Publics MS-SQL Allowed Grants to Public MYSQL Allowed Grants to Public Netezza Allowed Grants to Public Oracle Allowed Grants to Public Postgres Allowed Grants to Public Teradata Allowed Grants to Public	TUPLA, Objeto/Mandato Aplicación 8 (Asesoramiento de seguridad) Lista de objetos/mandatos para los que se permiten otorgamientos a public. Estos objetos se omitirán en pruebas de MS-SQL y Sybase que comprueban los otorgamientos a public. Nota: El grupo de excepciones puede contener una expresión regular o sólo un miembro. Si es una expresión regular, el miembro de grupo debe empezar por (R) (sensible a mayúsculas y minúsculas), y los registros en el detalle se comprobarán con la expresión regular a continuación de la (R). Por ejemplo, si un miembro de grupo es: (R)SYSTEM.[a-z]+ cada registro de detalle se comprobará utilizando el patrón: SYSTEM.[a-z]+ Si el miembro no empieza por (R), el registro de detalle se considerará una excepción sólo si es igual al miembro de grupo. Tenga en cuenta que un grupo puede contener una combinación de expresiones regulares y excepciones específicas.
Creador de asesoramientos de seguridad	MS-SQL Extended Procedures Allowed	El tipo de grupo es Objetos
Creador de asesoramientos de seguridad	Administradores de base de datos MS-SQL	El tipo de grupo es Usuarios
Creador de asesoramientos de seguridad	Perfil de Teradata	El tipo de grupo es Objetos
Público	Mandatos de gestión de cuentas	Mandatos utilizados para mantener las cuentas (usuarios, roles, permisos), por ejemplo: REVOKE, GRANT, ALTER/CREATE/DROP USER
Público	Procedimientos de gestión de cuentas	Objetos de gestión de cuentas, procedimientos almacenados utilizados para mantener las cuentas (usuarios, roles, permisos)
Público	Usuarios activos	El tipo de grupo es Usuarios
Público	Usuarios de administración	Usuarios administrativos predeterminados (DBA y SysAdmins)
Público	Objetos de administración	Objetos con privilegios, objetos a los que sólo pueden acceder las cuentas de DBA o Sys. De forma predeterminada, estas cuentas están bloqueadas para "public".
Público	Mandatos administrativos	Mandatos con privilegios, que sólo deberían ejecutar los DBA. Por ejemplo: mandatos GRANT, BACKUP, DDL
Público	Programas administrativos	Programas de utilidad de base de datos (clientes) que vienen con la base de datos y normalmente residen en el servidor de base de datos y podría utilizar el propio servidor
Público	Mandatos ALTER	Por ejemplo: alter database, alter procedure, alter profile, alter session, alter user
Público	Mandatos con privilegios de la aplicación	Mandatos con privilegios públicos que se deberían revocar de "public", pero no se revocan ya que los utiliza la aplicación

SQL_APP_NAME	GROUP_DESCRIPTION	MEMBERS
Público	Procedimientos con privilegios de la aplicación	Objetos con privilegios de la aplicación que se deberían revocar de "public" pero no se revocan ya que los utiliza la aplicación
Público	Usuarios del esquema de aplicaciones	Usuarios de aplicaciones, usuario de base de datos creado por la aplicación para mantener/utilizar las tablas de aplicación
Público	Candidatos de archivado	El tipo de grupo es Objetos
Público	Programas fuente autorizados	El tipo de grupo es Programas fuente
Público	Usuarios autorizados	El tipo de grupo es Usuarios
Público	Lista de perfilado de conexión	El tipo de grupo es IP de cliente/Aplic. Orig./Usuario BD/IP servidor/Nombre serv. Lista de conexiones permitidas
Público	Mandatos CREATE	Por ejemplo: create context, create database link, create function, create statistics, create type, create user
Público	Entidades relacionadas con credenciales	Tipos de auditoría de Guardium, Autosupervisión, por ejemplo, allowed_role, LDAP_config, Turbine_user_group_role
Público	Mandatos de transferencia de datos	Mandatos de copia de seguridad, mandatos que realizan la copia de seguridad/restauración de datos de base de datos
Público	Procedimientos de transferencia de datos	Objetos de transferencia de datos, procedimientos que realizan la copia de seguridad/restauración de datos de base de datos (principalmente en MSS y SYB)
Público	Usuarios predefinidos de BD	Usuarios predefinidos que no sean administradores o todos los usuarios predefinidos, incluidos los usuarios administrativos
Público	Mandatos DBCC	El tipo de grupo es Mandatos
Público	Mandatos DDL	Lenguaje de definiciones de datos, mandatos con privilegios de esquema, por ejemplo, ALTER, CREATE, DROP
Público	Mandatos DML	Mandatos DML, por ejemplo, insert, truncate, update
Público	Mandatos DROP	Por ejemplo, drop_context, drop_event_monitor, drop_procedure, drop_role
Público	Todos los objetos/campos de DW Todos los objetos de DW Objetos accedidos de DW Execute Objetos accedidos de DW Select Objetos/campos accedidos de DW Select	Hay cinco informes predefinidos que utilizan datos supervisados para mostrar los nombres de objeto. Todos estos informes empiezan por el prefijo DW (Data Warehouse). Consulte el tema de ayuda sobre cómo informar sobre tablas/columnas latentes para obtener información adicional sobre cómo utilizar estos informes predefinidos.
Público	Servidores de aplicaciones EBS	El tipo de grupo es IP de cliente
Público	Servidores de BD de EBS	El tipo de grupo es IP de servidor
Público	Mandatos EXECUTE	Por ejemplo: call, execute, execute function
Público	Mandatos GRANT	Por ejemplo: grant, grant objectives, grant system privileges
Público	Categorías de auditoría de Guardium para informes detallados	Parches de Guardium, TURBINE_USER_GROUP_ROLE
Público	Servidores de aplicaciones de ICM	El tipo de grupo es IP de cliente
Público	Servidores de BD de ICM	El tipo de grupo es IP de servidor
Público	ImportLDAPUser	El tipo de grupo es Objetos
Público	ImportLDAPUser_bindValues	El tipo de grupo es Objetos
Público	Entidades de motor de inspección	Por ejemplo: adminconsole_sniffer, software_tap_db_client, software_tap_db_server
Público	Mandatos de Java™	Por ejemplo: alter java, create java, drop java
Público	Mandatos KILL	Por ejemplo: kill
Público	Masked_SP_Executions_MS_SQL_SERVER	Para MS SQL Server, un grupo que incluye un conjunto de nombres de procedimientos almacenados (SP). Si hay una ejecución de un procedimiento incluido, todo se enmascarará, incluso si está entre comillas. Está predefinido como vacío.
Público	Masked_SP_Executions_Sybase	Para Sybase, un grupo que incluye un conjunto de nombres de procedimientos almacenados (SP). Si hay una ejecución de un procedimiento incluido, todo se enmascarará, incluso si está entre comillas. Está predefinido como vacío.
Público	Mandatos Skip de MongoDB	El tipo de grupo es Mandatos
Público	Procedimientos de replicación de MS-SQL	El tipo de grupo es Objetos
Público	Procedimientos del sistema de seguridad de MS-SQL	El tipo de grupo es Objetos
Público	Procedimientos del sistema de MS-SQL	El tipo de grupo es Objetos

SQL_APP_NAME	GROUP_DESCRIPTION	MEMBERS
Público	Objetos confidenciales HRMS de Oracle EBS	El tipo de grupo es Objetos
Público	Oracle EBS-PCI	El tipo de grupo es Objetos
Público	Oracle EBS-SOX	El tipo de grupo es Objetos
Público	Usuarios predefinidos de Oracle	El tipo de grupo es Usuarios
Público	Mandatos de asociación de iguales	Los mandatos que realizan enlaces/replicaciones de datos, por ejemplo, enlaces, envío de registros, replicaciones, instantáneas
Público	Procedimientos de asociación de iguales	Objetos de asociación de iguales, procedimientos que realizan enlaces/replicaciones de datos Por ejemplo: Enlaces, envío de registros, replicaciones, instantáneas
Público	Objetos de PeopleSoft	El tipo de grupo es Objetos
Público	Objetos confidenciales de PeopleSoft	El tipo de grupo es Objetos
Público	Mandatos de rendimiento	Por ejemplo: analyze, create statistics, update all statistics
Público	Entidades relacionadas con política	Por ejemplo, access_rule, gdm_install_policy_header
Público	Objetos de desbordamiento potencial	El tipo de grupo es Objetos
Público	Mandatos de procedimientos	Por ejemplo: begin, call, execute, exit, repeat, set
Público	PROCEDURE DDL	Por ejemplo: alter procedure, create procedure, drop procedure
Público	Servidores de aplicaciones de PSFT	El tipo de grupo es IP de cliente
Público	Servidores de BD de PSFT	El tipo de grupo es IP de servidor
Público	Procedimientos ejecutables públicos	Objetos de sólo ejecución, procedimientos/funciones/paquetes que de forma predeterminada han otorgado acceso a public
Público	Objetos seleccionables públicos	Objetos de sólo selección, tablas que se forma predeterminada han otorgado acceso a public
Público	Mandatos RESTORE	Por ejemplo: restore database, restore log
Público	Mandatos REVOKE	Por ejemplo: revoke object privileges, revoke system privileges
Público	Mensajes de error indicativos de riesgo	Errores de SQL relacionados con la seguridad
Público	Servidores Sharepoint	
Público	SAP-PCI	El tipo de grupo es Objetos
Público	Servidores de aplicaciones de SAP	El tipo de grupo es IP de cliente
Público	Servidores de BD de SAP	El tipo de grupo es IP de servidor
Público	Objetos confidenciales HR de SAP	El tipo de grupo es Objetos
Público	Mandato Select	Por ejemplo: select, select list
Público	Objetos confidenciales	Por ejemplo: actividad, ventas
Público	Servidores de aplicaciones de SIEBEL	El tipo de grupo es IP de cliente
Público	Servidores de BD de SIEBEL	El tipo de grupo es IP de servidor
Público	Objetos confidenciales SIA de Siebel	El tipo de grupo es Objetos
Público	Programa fuente CASO ESPECIAL	El tipo de grupo es Programas fuente
Público	Objetos sospechosos	El tipo de grupo es Objetos
Público	Usuarios sospechosos	El tipo de grupo es Usuarios
Público	Mandatos de configuración del sistema	Mandatos de configuración de base de datos (un subconjunto de Mandatos administrativos) Por ejemplo: ALTER DATABASE, ALTER SYSTEM
Público	Procedimientos de configuración del sistema	Objetos de configuración del sistema (un subconjunto de Objetos de administración)
Público	Usuarios de BD finalizados	El tipo de grupo es Usuarios
Público	Objetos vulnerables (con comodines)	Objetos de base de datos de los que se han informado vulnerabilidades
Público	Verbos de compartición de archivos de Windows	El tipo de grupo es Mandatos

SQL_APP_NAME	GROUP_DESCRIPTION	MEMBERS
Público	Usuarios predeterminados de DB2 Usuarios predeterminados de IBM iSeries Usuarios predeterminados de Informix Usuarios predeterminados de MS-SQL Server Usuarios predeterminados de MYSQL Usuarios predeterminados de Netezza Usuarios predeterminados de Oracle Uxsuarios predeterminados de PostgreSQL Usuarios predeterminados de Sybase Usuarios predeterminados de Teradata	El tipo de grupo es Usuario de BD/Contraseña de BD
Público	Mandatos Skip de Hadoop Objetos Skip de Hadoop No servidor Hadoop	El tipo de grupo es Mandato El tipo de grupo es Objeto El tipo de grupo es IP de servidor
Público	Reproducir - Excluir de comparación Reproducir - Incluir en comparación	El tipo de grupo es Objetos
Creador de procesos de auditoría		Está predefinido como vacío.
Creador de línea base		Está predefinido como vacío. Atención: El Creador de línea base y su funcionalidad está en desuso desde Guardium V10.1.4.
Clasificador		Está predefinido como vacío.
Seguridad exprés		Está predefinido como vacío.

Tema principal: Grupos

Roles de seguridad

Se utilizan roles de seguridad para otorgar acceso a los datos (grupos, consultas, informes, etc.) y otorgar acceso a aplicaciones (Creador de grupos, Creador de informes, Creador de políticas, CAS, Asesoramientos de seguridad, etc).

De forma predeterminada, cuando se define inicialmente un componente, sólo el propietario (la persona que lo ha definido) y el usuario de administración (que tiene privilegios especiales) tienen permiso para acceder y modificar dicho componente.

Puede permitir que otros usuarios accedan a los componentes que defina asignando roles de seguridad. Por ejemplo, si asigna un rol de seguridad denominado DBA a un proceso de auditoría, todos los usuarios asignados al rol DBA podrán acceder a ese proceso de auditoría.

Nota: Para configurar la importación de usuarios de LDAP, el usuario accessmgr debe tener el privilegio para ejecutar el Creador de grupos. En determinadas situaciones, cuando se realizan cambios en el privilegio de rol, se puede eliminar el privilegio de accessmgr a Creador de grupos. Como consecuencia, resulta imposible guardar o ejecutar con éxito una importación de usuarios de LDAP. Vaya al portal de gestión de acceso y seleccione Permisos de rol. Elija la aplicación Creador de grupos y asegúrese de que haya una marca de selección en todos los recuadros de rol o una en el recuadro accessmgr.

Asignar roles de seguridad

1. Abra o seleccione el elemento al que desea asignar uno o varios roles de seguridad (por ejemplo, una definición de informe o política).
2. Pulse Roles.
3. Seleccione todos los roles que desee asignar en la lista Asignar roles de seguridad. Sólo puede asignar roles que estén asignados a su cuenta.
4. Pulse Aplicar.

Definir un rol de seguridad nuevo

De forma predeterminada, sólo el usuario accessmgr tiene permiso para crear o eliminar roles de seguridad.

1. Inicie sesión como accessmgr y abra el Navegador de rol de usuario pulsando Acceso > Gestión de acceso > Navegador de rol de usuario.
2. Al final del navegador de rol, pulse Añadir rol.
3. En el panel Formulario de rol, especifique un nuevo Nombre de rol y pulse Añadir rol.

Eliminar un rol de seguridad

De forma predeterminada, sólo el usuario accessmgr tiene permiso para crear o eliminar roles de seguridad. Para eliminar un rol asignado a un componente, consulte Asignar roles de seguridad a un componente.

1. Inicie sesión como accessmgr y abra el Navegador de rol de usuario pulsando Acceso > Gestión de acceso > Navegador de rol de usuario.
2. Pulse Suprimir para cualquier rol y, a continuación, pulse Confirmar supresión.

Tema principal: Gestión del sistema Guardium

Notificaciones

Utilice el Alertador y el Creador de alertas para crear notificaciones. Cuando se requieran notificaciones por correo electrónico u otras para acciones de alerta, siga este procedimiento para cada tipo de notificación que se vaya a definir.

Configuración del alertador

1. Antes de elegir las acciones de alerta, debe configurar los valores SMTP de correo electrónico en el Alertador
2. Abra el Alertador pulsando Proteger > Detección de intrusión en base de datos > Alertador.
3. Rellene la información de SMTP y/o SNMP.
4. Después de rellenar cada sección, pulse Probar conexión y verifique que la conexión funciona. Recibirá un mensaje que indicará que no se puede localizar la conexión si la conexión no funciona.
5. Pulse Aplicar para guardar la configuración.
6. Como mínimo se debe especificar la dirección IP/nombre de host, el puerto y la dirección de correo electrónico de retorno.
7. Seleccione *Correo* en el menú Tipo de notificación. Si la gravedad del mensaje es *ALTA*, se establece un distintivo Urgente.
8. Seleccione un usuario (que puede ser una persona o un grupo) en la lista Receptor de alertas. Los receptores adicionales para notificación por correo electrónico en tiempo real son Invocador (el usuario que ha iniciado el mandato de SQL real que ha causado el desencadenante de la política) y Propietario (el propietario o propietarios de la base de datos). El invocador y el propietario se identifican recuperando los ID de usuario (basados en IP) configurados mediante las API de Guardium.
9. Pulse Añadir.

Crear una alerta

1. Tras configurar el Alertador, abra el Creador de alertas pulsando Proteger > Detección de intrusión en base de datos > Creador de alertas.
2. Rellene la información en las secciones Valores, Definición de alerta, Umbral de alerta y Notificación y pulse Aplicar.
3. Elija quién recibirá las notificaciones pulsando Añadir receptor... y eligiendo un usuario.

Tema principal: Gestión del sistema Guardium

Cómo crear una alerta en tiempo real

Envíe una alerta en tiempo real al administrador de base de datos siempre que haya más de tres inicios de sesión fallidos para el mismo usuario en un plazo de cinco minutos.

Acerca de esta tarea

Genere alertas de seguridad en tiempo real cada vez que se detecte actividad sospechosa o se infrinjan las políticas de acceso.

Siga estos pasos:

1. Cree una política
2. Añada reglas a la política
3. Instale la política
4. Configure una alerta en tiempo real cuando se ejecute la política

Requisitos previos

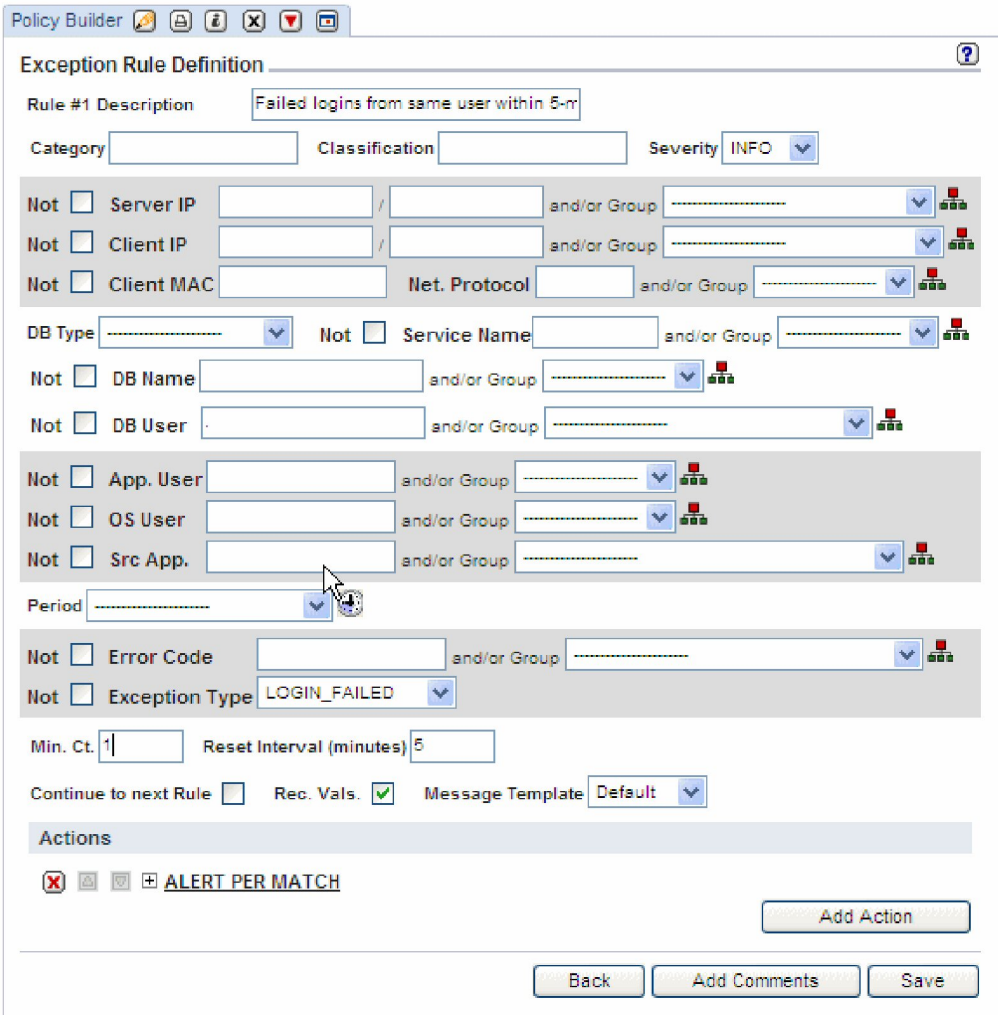
Configure SMTP en el Alertador. Abra el Alertador pulsando Proteger > Detección de intrusión en base de datos > Alertador y a continuación rellene la información de SMTP.

Nota: Las infracciones de política también se pueden ver como un informe en Gestión de incidentes. Consulte Políticas para obtener completa información.

Procedimiento

1. Cree una política.
   a. Abra el Creador de políticas pulsando Configuración > Herramientas y vistas > Creador de políticas para datos o aplicaciones.
   b. Pulse Nuevo o modifique una política existente seleccionando el Buscador de políticas y pulsando Modificar.
   c. Rellene la información necesaria y pulse Aplicar para guardar la política.
2. Añada las reglas a la política.
   a. Después de guardar la política, pulse Editar reglas para ver las reglas de política existentes.
   b. Pulse Añadir reglas... y a continuación podrá elegir entre cinco reglas.
   c. Elija Añadir regla de excepción y rellene la información necesaria.

      La pantalla Definición de regla de excepción empieza con los elementos siguientes:



- Descripción: Especifique un nombre abreviado descriptivo de la regla.
- Categoría: Se registrará la categoría con las infracciones y se utiliza para la creación de grupos e informes. Si no se especifica nada, se utilizará el valor predeterminado de la política.
- Clasificación: Especifique una clasificación (opcional). Como la categoría, se registra con las excepciones y se puede utilizar para la creación de grupos e informes.
- Gravedad: Seleccione un código de gravedad en el menú: INFORMACIÓN, BAJA, NINGUNA, MEDIA o ALTA (el valor predeterminado es INFORMACIÓN).

d. Utilice los demás campos para especificar cómo correlacionar la regla: dónde buscar, qué buscar, a quién buscar y cuándo buscar.
e. Especifique un punto "." en el campo Usuario de BD para contabilizar cada valor individual por separado.
f. En el menú Tipo excep. (tipo de excepción), seleccione LOGIN_FAILED.
g. Utilice el Recuento mínimo para establecer el número mínimo de veces que la regla debe coincidir antes de que se desencadene la acción. Para este ejemplo, elija 1. El número de veces que se ha cumplido se restablecerá cada vez que se desencadene la acción o cuando caduque el intervalo de restablecimiento.
h. Utilice el Intervalo de restablecimiento para establecer el número de minutos tras los cuales el contador de la regla se restablecerá a cero. El contador también se restablece a cero cada vez que se desencadena una acción de regla. Para este ejemplo, elija 5.
i. Marque el recuadro de selección Cont. a regla siguiente para continuar probando reglas una vez que se haya cumplido esta regla y se haya desencadenado su acción. Si no está seleccionado, no se probarán reglas adicionales cuando se cumpla esta regla.
j. Marque el recuadro de selección Val. Grab. para indicar que cuando se desencadene la acción de regla se registrará toda la sentencia SQL que causa este suceso y estará disponible en el informe de infracción de política. Si no se marca, el atributo Serie SQL estará vacío.

3. Añada una acción cuando se desencadene la regla.
   a. En la sección Acciones de la pantalla Definición de regla de excepción, pulse Añadir acción.
   b. Seleccione una opción en el menú Acción y pulse Aplicar. Para este ejemplo, elija *ALERTA POR COINCIDENCIA* para obtener una notificación cada vez que se ejecuta la regla.
   c. Seleccione una opción en el menú Tipo de notificación. Debe configurar el Alertador para tipos de notificación SNMP o correo.
   d. Añada un receptor de alertas y pulse Aplicar para guardar la acción.
4. Instale la política.
   a. Pulse Configuración > Herramientas y vista > Instalación de políticas.
   b. Busque la política en el menú Instalador de políticas, seleccione una acción de instalación y pulse Modificar planificación o Ejecutar una vez ahora. Ahora la política está instalada. El receptor de alertas recibirá notificaciones en tiempo real cuando se ejecuten reglas de política.

Tema principal: Gestión del sistema Guardium

Administración de clase de alerta personalizada

Utilice una clase de alerta personalizada para enviar alertas a un destinatario personalizado. Suba la clase personalizada y, a continuación, utilice el Creador de alertas para designar la clase personalizada como un receptor de notificaciones de alerta.

- Para utilizar una clase personalizada, primero debe subirla al sistema Guardium. Pulse Configuración > Clases personalizadas > Alertas > Subir clase de alerta para subir una clase de creación de alertas personalizada. Pulse Examinar para seleccionar un archivo y a continuación Aplicar para guardar.
- Después de subir la clase personalizada, utilícela en una alerta con el Creador de alertas. Abra el Creador de alertas pulsando Gestionar > Detección de intrusión en base de datos > Creador de alertas. Rellene la información necesaria, seleccione *CUSTM* en el menú Tipo de notificación y pulse Guardar.

Tema principal: Gestión del sistema Guardium

Alertas predefinidas

Tabla que describe las alertas predefinidas que se encuentran en el Creador de alertas.

Guardium se proporciona con un conjunto de alertas predefinidas que se pueden encontrar en el Creador de alertas. Abra el Creador de alertas pulsando Proteger > Detección de intrusión en base de datos > Creador de alertas. Cuando abra el Creador de alertas, se le presentará una lista de todas las alertas existentes en el Buscador de alertas. Seleccione una alerta en el buscador y pulse Modificar para editarla.

En la pantalla Modificar alerta, modifique cualquier parte de la alerta, por ejemplo, receptores o umbral.

No puede modificar las consultas predeterminadas en las que se basan las alertas. Si desea modificar una consulta, pulse el icono Editar esta consulta para cualquier consulta para abrir el Creador de consultas. Una vez en el creador, clone cualquier consulta y a continuación modifique el clon para que se ajuste a sus necesidades.

Tras realizar los cambios en una alerta, pulse Aplicar para guardarlos.

La tabla siguiente describe todas las alertas predefinidas.

Tabla 1. Alertas predefinidas

Alerta	**Descripción**
S-TAP activos modificados	Comprueba si hay cambios en los motores de inspección de S-TAP activos durante el último intervalo de acumulación. La alerta se desencadenará si se ha cambiado al menos un motor de inspección durante el periodo. De forma predeterminada, la alerta realiza la comprobación cada 1/2 hora y comprueba la última hora.
Errores de Agregación/Archivado	Alerta una vez al día sobre todas las tareas de agregación o archivado que no se han completado correctamente.
Alerta de perfilado de conexión	La alerta se ejecuta cada 60 minutos y envía aviso al grupo predefinido, la Lista de perfilado de conexión - Lista de nombres de conexiones permitidas
Cambios en la configuración de instancias de CAS	Alerta una vez al día sobre los cambios de configuración de instancia de CAS.
Cambios de plantilla de CAS	Alerta una vez al día sobre los cambios de configuración de plantilla de CAS.
Cambios de origen de datos	Alerta una vez al día sobre los cambios de definición de origen de datos.
Espacio de disco de base de datos	Alerta cada 10 minutos si la base de datos interna se llena más del 80 % . Consulte el tema de ayuda Autosupervisión para obtener más información sobre el espacio de disco (% lleno) y el proceso Nanny de Guardium.
No tráfico empresarial	La alerta No tráfico empresarial se ejecuta sólo en sistemas de Gestor central. Se basa en una consulta similar a la consulta en la alerta Sin tráfico y recupera los registros con: indicación de fecha y hora entre X y Y, donde X es un parámetro de consulta e Y es una consulta generada por el mecanismo de alerta en función del intervalo de acumulación (de la misma forma en que funciona la alerta Sin tráfico existente).
S-TAP de empresa modificados	Esta alerta sólo se ejecutará en sistemas de Gestor central.
Inicios de sesión fallidos en Guardium	Cada 10 minutos alerta si hay más de 5 intentos de inicio de sesión fallidos en el dispositivo de Guardium.
Guardium - Añadir/eliminar usuarios	Alerta una vez al día si se ha añadido o eliminado algún usuario de Guardium.
Guardium - Actividad de credenciales	Alerta una vez al día si se han producido cambios de credenciales de Guardium, incluidos cambios de configuración de LDAP.
Unidad gestionada inactiva	La alerta se ejecuta 30 minutos y envía un aviso una vez al día al grupo predefinido denominado "Alerta de unidades gestionadas".
S-TAP inactivos desde	Alerta una vez cada hora sobre todos los S-TAP de los que no se tienen noticias.
Motores de inspección y S-TAP	Alerta una vez al día sobre la actividad relacionada con la configuración de S-TAP y el motor de inspección.
Sin tráfico	Alerta para indicar si no hay tráfico de los servidores de base de datos específicos. Esta alerta avisará si no se recopila tráfico de un servidor del que el sistema Guardium estaba recopilando tráfico en algún momento durante las últimas 48 horas. La alerta se desencadenará cuando no haya tráfico en el periodo definido en el intervalo de acumulación. Por ejemplo, si el intervalo de acumulación es 60 minutos, la alerta enviará un correo electrónico si no ha habido tráfico de un servidor de base de datos específico en la última hora pero ha habido tráfico en las últimas 48 horas. La alerta enviará un correo electrónico (de forma predeterminada) sólo cada 24 horas. Los parámetros como intervalo de acumulación, intervalo de notificación, frecuencia de ejecución etc. se pueden personalizar. Los parámetros como umbral, por línea, operador, consulta, etc. no se deberían cambiar, ya que si se cambian estos parámetros la alerta no funcionará correctamente. Tenga en cuenta que la consulta Sin tráfico no se debe clonar.
Sin tráfico por el servidor y el protocolo	Es similar a la alerta Sin tráfico regular con las diferencias siguientes: La alerta es por nombre de servicio/protocolo de red, y se notificará por línea. Hay un nuevo parámetro adicional: Intervalo de tráfico activo, que determina cuándo se ha recibido la última solicitud de cada servidor. La alerta se desencadenará en las condiciones siguientes: No ha habido ningún tráfico durante el intervalo de alerta de cada servidor/protocolo de red pero ha habido tráfico desde: Intervalo de tráfico activo para esa combinación. Diferente de la alerta Sin tráfico regular que se desencadenará si no hay tráfico durante el intervalo de alerta pero ha habido tráfico en las 48 horas anteriores por IP servidor.
Alertar sobre cambios de política	Alerta una vez al día si ha habido cambios de política de seguridad.
Consultas ejecutándose por largo tiempo	Notifica si una consulta tarda más de 900 segundos en ejecutarse.

Alerta	Descripción
Excepciones de trabajos planificados	Alerta cada 10 minutos sobre cualquier excepción de trabajo planificado (incluidos los trabajos de asesoramiento).

Tema principal: Gestión del sistema Guardium

Planificación

El planificador de uso general se utiliza para planificar muchos tipos diferentes de tareas (archivado, agregación, automatización de flujo de trabajo, etc.) .

En función del tipo de tarea que se esté realizando, es posible que no todas las características que se describen aquí estén disponibles; por ejemplo, las planificaciones para algunos tipos de tareas se pueden poner en pausa, mientras que otras no (sólo se pueden detener o iniciar).

Nota: Tenga en cuenta las anomalías de planificación que se pueden producir al planificar tareas durante el horario de verano.

Definir o modificar una planificación

1. En una tarea (por ejemplo, Creador de procesos de auditoría), pulse Definir planificación o Modificar planificación para abrir el panel Definición de planificación.
2. Rellene la hora de inicio. El valor predeterminado es 12 a.m. (medianoche).
3. Opcionalmente, para ejecutar la tarea más de una vez al día:
   - Seleccione un valor en la lista Reiniciar (cada hora hasta cada 12 horas). El valor predeterminado es Ejecutar sólo una vez, lo que significa que la tarea no se reiniciará durante el día.
   - Seleccione un valor en la lista Repetir (cada minuto hasta cada 59 minutos). El valor predeterminado es No repetir.
4. En la lista Planificar por, seleccione una de las opciones siguientes:
   - Día/Semana para definir una planificación basada en uno o varios días de la semana (Lunes, Martes, Miércoles, etc.) .
   - Mes para definir una planificación basada en uno o más días del mes, para cada mes o meses específicos.

   Si ha seleccionado Día/Semana en la lista Planificar por, marque cada día de la semana en que desea que se ejecute la tarea, o pulse Todos los días para seleccionar todos los días (o para desmarcar todos los días si ya están seleccionados).

   O BIEN

   Si ha seleccionado Mes en la lista Planificar por, realice una de las acciones siguientes:

   - Para seleccionar un día numerado (el 15, por ejemplo):
     - Seleccione el botón Día.
     - Seleccione un día: 1-31, según el mes seleccionado.
     - Seleccione Cada mes o uno o varios meses específicos.
   - Para seleccionar una aparición de día de la semana en el mes (el primer lunes, por ejemplo):
     - Seleccione el botón.
     - Seleccione una semana relativa al inicio del mes: primera, segunda, tercera, etc.
     - Seleccione un día de la semana: domingo, lunes, martes, etc.
     - Seleccione Cada mes o uno o varios meses específicos.
5. En la lista Hora de inicio planificada, seleccione la hora y minuto cuando desea ejecutar la tarea. Si se elige una hora anterior a AHORA, la Hora de inicio del planificador cambiará a AHORA.
6. Pulse Aplicar.

Pausar una planificación

Nota: Tenga en cuenta que no todos los tipos de tareas planificadas proporcionan una opción de pausa.

1. Pulse Poner en pausa.
2. Confirme la acción.

Eliminar una planificación

Una vez que se ha definido una planificación, el botón Eliminar aparece en el panel Definición de planificación.

1. Pulse Definir planificación o Modificar planificación para abrir el panel Planificar definición.
2. Pulse el botón Suprimir.

Tema principal: Gestión del sistema Guardium

Alias

Cree sinónimos para valores de datos u objetos que se utilizarán en informes o consultas.

Visión general de alias

Se utiliza un alias para mostrar un nombre descriptivo o fácil de usar para un valor de datos.

Por ejemplo, podría definirse *Servidor financiero* como un alias de la dirección IP 192.168.2.18. Una vez que se ha definido un alias, los usuarios pueden visualizar resultados de informe, formular consultas y especificar valores de parámetros utilizando el alias en lugar del valor de datos.

Se pueden definir alias de distintas formas:

- Mediante la herramienta Creación de alias IP-Nombre de host: Utilice esta herramienta para generar alias para las IP de cliente y servidor descubiertas.

  Pulse Proteger > Detección de intrusión en base de datos > Creación de alias IP-Nombre de host para abrir la herramienta Creación de alias IP-Nombre de host.

- Mediante el Creador de alias: Utilice este método para definir alias manualmente.

Abra el Creador de alias pulsando Cumplir > Herramientas y vistas > Creador de alias.

- Mediante una consulta.
- Cuando se utiliza el Creador de grupos, con la Definición rápida de alias.
-

Nota: Los cambios de alias en el Gestor Central o las unidades gestionadas no estarán disponibles en otros sistemas hasta que se reinicie la interfaz gráfica de usuario o los cambios de alias se realicen mediante la interfaz gráfica de usuario.

Creación de alias IP-Nombre de host

Una de las aplicaciones más comunes de los alias es su uso como sinónimos de direcciones IP. Utilice esta herramienta para planificar el descubrimiento de IP de cliente y servidor y generar alias para ellas.

1. Abra la herramienta Creación de alias IP-Nombre de host pulsando Proteger > Detección de intrusión en base de datos > Creación de alias IP-Nombre de host.
2. Marque el recuadro de selección Generar alias de nombre de host para IP de cliente y servidor (si están disponibles).
3. Marque el recuadro de selección Actualizar alias de nombre de host existentes si se redescubren si desea que la herramienta busque y actualice alias continuamente.
4.
5. Pulse Aplicar para guardar la configuración y, a continuación, planificar la operación.
   - Pulse Ejecutar una vez ahora para iniciar la herramienta inmediatamente.
   - Pulse Definir planificación... para planificar la herramienta en el futuro.
   - Pulse Pausar para pausar la generación de los alias de IP de cliente y servidor.

Creador de alias

Utilice este método para crear manualmente un alias.

1. Abra el Creador de alias pulsando Configuración > Herramientas y vistas > Creador de alias.
2. Seleccione el tipo de atributo para el que desea definir alias.
3. Filtre la búsqueda por ese tipo de atributo utilizando los campos Valor y Alias y pulse Buscar.
4. Si hay resultados que coinciden con su búsqueda, se mostrarán en la tabla de valores y alias. Pulse Aplicar para los resultados de la búsqueda, o añada un nuevo alias especificando un Valor y nombre de Alias y pulsando Añadir.
5. Añada un comentario a un alias pulsando el icono Comentarios de elemento . Esto puede resultar útil para consultar rápidamente en el futuro a qué hace referencia un alias.

Definir alias utilizando una consulta

Utilice este método para crear alias a partir de una consulta. Cuando se ha subido una tabla personalizada a Guardium, esa tabla se puede utilizar para correlacionar alias con valores específicos.

1. Abra el Creador de alias pulsando Configuración > Herramientas y vistas > Creador de alias.
2. Seleccione el tipo de atributo para el que desea definir alias en el Buscador de alias y pulse Cumplimentar desde consulta para abrir el panel Creador de alias desde configuración de consulta.
3. Rellene la información necesaria y pulse Guardar para guardar el alias.
   - Seleccione la consulta que se ejecutará en el menú Consulta.
   - Elija un valor para Elegir columna para columna de valor y Elegir columna para columna de alias.
   - Cuando ha seleccionado los valores de columna, se muestran más campos que debe cumplimentar (Desde fecha, Hasta fecha, Origen remoto y cualquier parámetro adicional para la consulta seleccionada).
   - Marque el recuadro de selección Borrar miembros de grupo existentes antes de importar para suprimir el contenido existente del grupo antes de completar desde la consulta.
   - Pulse Guardar para guardar.
   - Con la consulta guardada, los botones Planificación se activarán. Pulse Modificar planificación para ejecutar la consulta en el futuro, o pulse Ejecutar una vez ahora para ejecutarla inmediatamente.

Definición rápida de alias desde el Creador de grupos

Utilice este método para crear un alias para un grupo sobre la marcha durante la creación o llenado de un grupo.

1. Abra el Creador de grupos pulsando Configuración > Creador de grupos. Seleccione cualquier grupo de la lista y pulse Modificar.
2. Pulse Alias... para abrir la ventana Definición rápida de alias. Especifique un alias para cualquier grupo y guarde el alias pulsando Aplicar.

GuardAPI para alias

Utilice estos mandatos de GuardAPI para crear, actualizar y suprimir funciones de alias:

- grdapi create_alias
- grdapi update_alias
- grdapi delete_alias

Tema principal: Gestión del sistema Guardium
Información relacionada:
Configuración y gestión avanzadas del sistema Guardium (vídeo)

Fechas e indicaciones de fecha y hora

Utilice una herramienta de calendario para seleccionar una fecha exacta, y un selector de fecha relativa para seleccionar una fecha relativa a la hora actual.

Hay dos herramientas que se utilizan para rellenar los campos de fecha: una herramienta de calendario para seleccionar una fecha exacta y un selector de fecha relativa para seleccionar una fecha relativa a la hora actual (ahora -1 día, por ejemplo). Además, se pueden especificar manualmente fechas exactas o relativas.

Tenga en cuenta que al seleccionar o especificar fechas, es posible que la fecha del sistema en el que está ejecutando el navegador no sea la misma que la fecha en el dispositivo de Guardium al que está conectado.

Indicaciones de fecha y hora en las consultas

Es necesario tener cuidado al incluir las indicaciones de fecha y hora en las consultas.

En primer lugar, tenga en cuenta la distinción entre una indicación de fecha y hora (t minúscula) y una Indicación de fecha y hora (T mayúscula T).

- Una indicación de fecha y hora (t minúscula) es un tipo de datos que contiene un valor de fecha y hora combinado, que cuando aparece en pantalla se muestra siempre con el formato aaaa-mm-dd hh:mm:ss (por ejemplo, 2005-07-17 15:40:25). Cuando se crea o edita una consulta, la mayoría de los atributos con un tipo de datos de indicación de fecha y hora se visualizan con un icono de reloj en el panel Lista de entidades.
- Una indicación de fecha y hora (T mayúscula) es un atributo definido en muchos tipos de entidad. Suele contener la hora a la que se actualizó la entidad por última vez.

Si se incluye un valor de atributo Indicación de fecha y hora en una consulta, se generará una fila para cada valor de la indicación de fecha y hora. Esto puede producir una cantidad excesiva de salida. Para solucionar esto, utilice el agregador de recuento cuando incluya la indicación de fecha y hora en una consulta y, a continuación, detalle más en una fila de informe, para ver sólo los valores individuales de indicación de fecha y hora para los elementos incluidos en dicha fila, en un informe detallado. Consulte el apartado Campos agregados en consultas.

Cuando se muestra un valor de indicación de fecha y hora en una consulta que contiene atributos de indicación de fecha y hora en varias entidades, tenga cuidado de seleccionar el atributo de indicación de fecha y hora del tipo de entidad apropiado para el informe. Por ejemplo, si la consulta visualizará información de las entidades de cliente/servidor y de sesión, con la sesión seleccionada como la entidad principal, puede visualizar un atributo de indicación de fecha y hora de una o ambas entidades. Si incluye la indicación de fecha y hora de servidor/cliente, verá el mismo valor impreso para cada sesión para una conexión cliente-servidor determinada; siempre será la hora a la que se actualizó por última vez ese cliente/servidor específico. Si incluye el atributo Indicación de fecha y hora desde la sesión, verá la hora en que cada sesión listada se actualizó por última vez.

Sugerencia: Si el informe muestra horas que son todas la misma cuando espera que sean diferentes, es probable que haya incluido un atributo Indicación de fecha y hora de una entidad demasiado alta en la jerarquía de entidades para el nivel de detalle que desea en el informe.

Seleccionar una fecha exacta en el calendario

Para utilizar la ventana de calendario para seleccionar una fecha exacta:

1. Pulse el botón Calendario del campo donde desea insertar una fecha. Se abrirá un calendario en una ventana aparte.
   - Pulse en los botones de flecha para visualizar el mes anterior o siguiente en la ventana de calendario.
2. Pulse cualquier fecha para seleccionar ese día. La ventana de calendario se cerrará y la fecha seleccionada se insertará en el campo de fecha junto a la herramienta de calendario que se ha pulsado.
   Nota: La hora predeterminada de una fecha seleccionada utilizando el calendario es siempre 00:00:00 (el inicio del día). Para especificar cualquier otra hora del día, escriba sobre este valor, especificando la hora que desee en formato de 24 horas: hh:mm:ss, donde hh es la hora del día (0-23) y mm y ss son minutos y segundos, respectivamente (ambos 0-59).

Especificar manualmente una fecha exacta

1. Pulse el campo en el que desea especificar la fecha y escriba la fecha en formato aaaa-mm-dd, donde:
   - aaaa es opcional y puede ser cualquier valor entero positivo. Si se omite, el valor predeterminado de aaaa es el año actual. Si se especifica un año de uno o dos dígitos, la parte del siglo de la fecha toma el valor predeterminado 19.
   - mm es el mes (1-12)
   - dd es el día del mes (de 1 a 28, 29, 30 o 31, en función del mes)
2. Si no se especifica ninguna hora, la hora toma el valor predeterminado de 00:00:00 (el inicio del día). Para especificar cualquier otra hora del día, escriba sobre este valor, especificando la hora que desee en formato de 24 horas: hh:mm:ss, donde hh es la hora del día (0-23) y mm y ss son minutos y segundos, respectivamente (ambos 0-59).

Seleccionar una fecha relativa en el selector de fechas

En lugar de especificar una fecha exacta, a menudo es más conveniente especificar fechas relativas a la fecha actual (ahora) o a alguna otra fecha (por ejemplo, el primer lunes). Por ejemplo, para incluir siempre información de los siete días anteriores en una consulta, es más cómodo definir fechas relativas (por ejemplo, iniciar = ahora menos siete días y finalizar = ahora). La herramienta Selector de fechas relativas se puede utilizar para seleccionar una fecha relativa para muchos tipos de tareas.

1. Pulse el botón Selector de fechas relativas junto a cualquier campo en el que se permita una fecha relativa. Se abrirá la ventana Selector de fechas relativas.
2. Seleccione Ahora, Iniciar o Finalizar en la lista. Independientemente de su elección, la pantalla cambia para proporcionar selecciones adicionales.
3. En la lista central, seleccione este/a, último/a, o anterior, relativo a la unidad (día, semana, mes o día de la semana seleccionada en la lista siguiente) del modo siguiente:
   - Este/a es la unidad actual
   - Último es la unidad actual menos uno
   - Anterior es la unidad actual menos dos
4. Seleccione el día, semana, mes o un día específico: Lunes-Viernes.
5. Pulse el botón Aceptar cuando haya terminado. La fecha relativa se insertará en el campo situado junto al botón Selector de fechas relativas que se ha pulsado.
6.

Especificar manualmente una fecha relativa

Para especificar manualmente una fecha relativa, siga uno de los procedimientos. Las palabras clave no son sensibles a las mayúsculas y minúsculas, pero cada componente debe estar separado del siguiente por uno o más espacios.

Existen tres formatos generales que puede utilizar para especificar una fecha relativa:

AHORA menos un número especificado de minutos, horas, días, semanas o meses

O BIEN

El Inicio o Fin del día, semana o mes actual, último o anterior

O BIEN

El día de la semana pasado o anterior (domingo, lunes, martes, etc.)

Relativo a AHORA

1. Pulse el campo en el que desea especificar la fecha relativa.
2. Especifique la palabra clave AHORA.
3. Especifique un entero negativo que especifique el número relativo de horas, días, semanas o meses (no se permite ningún espacio entre el signo menos y el entero).
4. Especifique una palabra clave para las unidades utilizadas: HORA, DÍA, SEMANA o MES. Tenga en cuenta que el plural (horas, días, etc.) no está permitido. Ejemplo: ahora -14 día

Relativo a un día, semana o mes

1. Pulse el campo en el que desea especificar la fecha relativa.
2. Especifique las palabras clave INICIO DE o FIN DE.
3. Especifique ESTE o ÚLTIMO, seguido de DÍA, SEMANA o MES. Ejemplo: fin de última semana

Relativo a un día de la semana

1. Pulse el campo en el que desea especificar la fecha relativa.
2. Especifique las palabras clave INICIO DE o FIN DE.
3. Especifique ÚLTIMO o ANTERIOR, seguido de DOMINGO, LUNES, MARTES, MIÉRCOLES, JUEVES, VIERNES o SÁBADO. Ejemplo: inicio de martes anterior

Tema principal: Gestión del sistema Guardium

Periodos de tiempo

Utilice el Creador de periodos de tiempo para crear periodos de tiempo que se pueden utilizar para reglas de política y condiciones de consulta.

Cuando supervise la actividad de la base de datos, utilice los periodos de tiempo para especificar cuándo desea que se supervise. Utilice el Creador de periodos de tiempo para crear nuevos periodos de tiempo o modificar los existentes.

Añadir un periodo de tiempo

1. Vaya al Creador de periodos de tiempo pulsando Configuración > Herramientas y vistas > Creador de periodos de tiempo.
2. Expanda el panel Añadir periodo de tiempo pulsando el botón +.
3. Rellene la información y pulse Añadir para añadir el periodo de tiempo.
    - No incluya apóstrofos en la Descripción del periodo de tiempo.
    - Marque el recuadro de selección Contiguo para definir un único periodo de tiempo que puede abarcar varios días. Una semana laboral se define como contigua, mientras que un día laborable se define como no contiguo.

Eliminar un periodo de tiempo

1. Vaya al Creador de periodos de tiempo pulsando Configuración > Herramientas y vistas > Creador de periodos de tiempo.
2. Marque el recuadro de selección para el periodo de tiempo que desea eliminar y pulse Suprimir.

Tema principal: Gestión del sistema Guardium

Periodos de tiempo

Las reglas de política y las condiciones de consulta pueden probar los sucesos que se producen (o no) durante los periodos de tiempo definidos por el usuario.

Hay un conjunto de periodos de tiempo predefinidos (7x24, Trabajo después de horas laborables, Trabajo antes de horas laborables, Noche, Día laborable normal, Sábado, Domingo y Fin de semana), y los usuarios pueden definir los suyos propios.

Añadir un periodo de tiempo

1. Vaya al panel Periodo de tiempo:
    - Configuración> Herramientas y vistas > Creador de periodos de tiempo
2. Expanda el panel Añadir periodo de tiempo pulsando en el botón +.
3. Especifique una descripción exclusiva del periodo en el recuadro Descripción del periodo de tiempo. No incluya apóstrofos en la descripción.
4. Opcionalmente, marque el recuadro Contiguo para definir un único periodo de tiempo que puede abarcar varios días. Deje el recuadro desmarcado para definir un periodo de tiempo fijo en uno o más días.

   Ejemplo: Periodos de tiempo contiguos vs. no contiguos

   Los dos periodos de tiempo siguientes empiezan ambos a las 09:00 del lunes y finalizan el viernes a las 17:00:
    - Semana laborable se define como Contiguo.
    - Día laborable se define como No contiguo.

   El primer periodo de tiempo, Semana laboral, define un único periodo de 164 horas que empieza el lunes a las 9 AM y finaliza el viernes a las 5 PM, mientras que el segundo periodo de tiempo, Día laborable, define cinco periodos individuales de 8 horas (de 9 AM a 5 PM), de cinco días consecutivos (de lunes a viernes)

5. Especifique una hora de inicio en horas (00-24) y minutos (00-59) en el recuadro Desde hora.
6. Especifique una hora de finalización en horas (00-24) y minutos (00-59) en el recuadro Hasta hora.
7. Seleccione un día de inicio de la semana en el recuadro Desde día laborable.
8. Seleccione un día de finalización de la semana en el recuadro Hasta día laborable.
9. Opcionalmente, pulse el botón Comentarios para añadir comentarios (consulte Comentarios).

10. Pulse el botón Añadir.

Eliminar un periodo de tiempo

1. Vaya al panel Periodo de tiempo:
   - Configuración> Herramientas y vistas > Creador de periodos de tiempo
2. Marque el recuadro de selección Seleccionar para el periodo de tiempo que desea eliminar.
3. Pulse el botón Suprimir. Se le solicitará que confirme la supresión. Tenga en cuenta que no puede suprimir un periodo de tiempo utilizado por una regla de política existente.

Tema principal: Gestión del sistema Guardium

Comentarios

Los comentarios se aplican a definiciones y a resultados de proceso de flujo de trabajo.

Se pueden añadir y ver comentarios en varias ubicaciones de la interfaz de usuario. Puede añadir un comentario a un grupo o alias para fines de referencia, o añadir un comentario a un informe para facilitar los requisitos de auditoría. Por ejemplo, es posible que un auditor sepa por qué se ha hecho un cambio de configuración en una fecha determinada. Utilice un comentario para hacer referencia fácilmente al motivo por el que se ha realizado el cambio.

Los comentarios se aplican a definiciones (grupos, alias, informes, políticas) y a resultados de proceso de flujo de trabajo. Puede añadir varios comentarios a un componente, y puede añadir comentarios a comentarios, pero no puede modificar o suprimir comentarios existentes.

Hay dos clases distintas de comentarios:

- Las **entidades Comentarios** se almacenan en el Gestor central, y estarán disponibles en ese entorno del Gestor central, dadas las restricciones usuales sobre roles y permisos.
- Las **entidades Comentarios locales** se definen en una única unidad, y se mantienen locales a esa unidad. Los comentarios locales de la unidad autónoma o gestionada no se almacenan en el Gestor central.

Añadir o ver comentarios

1. Para ver los comentarios, abra la ventana Comentarios del usuario pulsando Cumplir > Informes > Comentarios del usuario.
2. En la interfaz de usuario, hay distintas maneras de añadir un comentario a una entidad o informe.
   - Añada un comentario a un grupo modificando el grupo y pulsando Añadir comentarios en la pantalla Gestionar miembros para grupo seleccionado.
   - Añada un comentario a un alias abriendo el Creador de alias y pulsando el icono Comentarios de elemento . Abra el Creador de alias pulsando Configuración > Herramientas y vistas > Creador de alias

Comentarios de informes

Vea un informe de todos los comentarios de usuario pulsando Cumplir > Informes > Comentarios del usuario.

- La entidad Comentarios locales se utiliza sólo en un entorno de Gestor central. Los comentarios locales permanecen locales para los sistemas en los que se han definido, y no se almacenan en el Gestor central.
- La entidad Comentarios contiene comentarios almacenados en el Gestor central.

Tema principal: Gestión del sistema Guardium

Cómo instalar parches

Instalar un único parche o varios parches como un proceso en segundo plano.

Acerca de esta tarea

Utilice este tema para proporcionar visibilidad y controlar la instalación, el estado, y el historial de parches.

Consulte Gestión central para obtener más información.

Este tema de procedimiento utiliza una combinación de mandatos de la CLI y las opciones de la interfaz gráfica de usuario para ayudarle a instalar el último parche de Guardium. Tras instalar un parche es necesario rearrancar el sistema Guardium.

Importante: Los parches bajados en formato ZIP se deben desempaquetar fuera del sistema Guardium antes de subirlos y de la instalación. Tenga en cuenta las siguientes restricciones para los parches con cambios en la estructura de la base de datos:

- Realice o planifique la instalación del parche cuando haya poca actividad en el sistema Guardium para evitar conflictos con procesos de larga ejecución como, por ejemplo, informes con mucha información, procesos de auditoría, copias de seguridad e importaciones.
- El tiempo exacto necesario para la instalación del parche depende de la utilización de la base de datos, la distribución de los datos y de otras consideraciones.
- Instale los parches de forma jerárquica, de arriba a abajo, aplicando primero los parches al gestor central, luego a los agregadores y por último a los recopiladores.

En el procedimiento siguiente, seguirá estos pasos desde el sistema Guardium designado y configurado como Gestor central:

1. Haga copia de seguridad del perfil del sistema, mediante el mandato de CLI store backup profile.
2. Especifique el mandato de CLI store system patch install para instalar un único parche o varios parches en el Gestor central desde una ubicación de red.
3. Pulse Configuración > Herramientas y vistas > Distribución de parches para mover los parches desde el Gestor central a las unidades gestionadas.

Procedimiento

Copia de seguridad del perfil del sistema

1. Utilizando un cliente SSH, inicie sesión en el Gestor central de IBM Security Guardium como usuario de la CLI.
2. Especifique el mandato siguiente: store backup profile

3. Aparecerá el siguiente recuadro de diálogo:

```
Do you want to setup for automatic recovery? (Y/n)
Enter the patch backup destination host:
Enter the patch backup destination directory:
Enter the patch backup destination user:
Enter the patch backup destination port if you have a special port for SCP operation, or press ENTER to use the default port:
Enter the patch backup destination password:
```

4. Utilice el siguiente mandato de CLI si la instalación del parche ha fallado, la reversión del parche ha fallado y la restauración automática ha fallado o se ha inhabilitado. El siguiente mandato obtiene el archivo de copia de seguridad previa al parche y lo restaura en el sistema. Si el archivo de copia de seguridad previa al parche se encuentra actualmente en el sistema, especifique el nombre del archivo. De lo contrario, para obtener el archivo se utiliza la información del perfil de copia de seguridad anterior al parche.

```
CLI>show backup profile patch backup flag is 1 patch backup automatic recovery flag is 1 patch backup dest host is
patch backup dest dir is patch backup dest user is patch backup dest port is patch backup dest pass is CLI>restore pre-patch
backup
```

Instale el parche o parches en el Gestor central

Nota: Un archivo de parche comprimido puede contener varios parches, pero sólo se puede instalar uno cada vez. Para instalar más de un parche, elija todos los parches que se deban instalar, separados por comas. Internamente, la CLI envía solicitudes para cada parche de la lista (en el orden especificado por el usuario) y el primer parche toma el tiempo de solicitud proporcionado por el usuario y cada parche posterior tres minutos después del anterior. Además, la CLI comprobará si ya se han solicitado los parches especificados y no permitirá solicitudes duplicadas.

5. Especifique el mandato siguiente:

```
store system patch install <tipo> <fecha> <hora>
```

donde <tipo> es sys, ftp, scp o cd y <fecha> y <hora> son la fecha y hora de la solicitud de la instalación del parche, con el formato AAAA-mm-dd y hh:mm:ss, respectivamente. Si no se especifica fecha y hora o si se especifica "ahora", la hora de la solicitud de instalación es AHORA.

Tabla 1. Descripciones y parámetros de los tipos de instalación de parche

Nombre	Descripción
sys	La opción sys se utiliza cuando se instala un segundo parche o parche subsiguiente desde un archivo comprimido que se ha copiado previamente en el sistema Guardium mediante este mandato. Utilice esta opción para aplicar un segundo parche o parche subsiguiente parche desde un archivo de parche que se ha copiado en el sistema IBM® Guardium mediante una ejecución anterior de store system patch. Instale desde /var/log/guard/patches

ftp o scp	Las opciones ftp y scp copian un archivo de parche comprimido desde una ubicación de red en el sistema Guardium. Para instalar un parche desde un archivo de parche comprimido ubicado en algún lugar de la red, utilice la opción ftp o scp, y responda a las solicitudes tal como se muestra a continuación.
	Importante: Los parches bajados en formato ZIP se deben desempaquetar fuera del sistema Guardium antes de subirlos y de la instalación. Tenga en cuenta las siguientes restricciones para los parches con cambios en la estructura de la base de datos:
	○ Realice o planifique la instalación del parche cuando haya poca actividad en el sistema Guardium para evitar conflictos con procesos de larga ejecución como, por ejemplo, informes con mucha información, procesos de auditoría, copias de seguridad e importaciones.
	○ El tiempo exacto necesario para la instalación del parche depende de la utilización de la base de datos, la distribución de los datos y de otras consideraciones.
	○ Instale los parches de forma jerárquica, de arriba a abajo, aplicando primero los parches al gestor central, luego a los agregadores y por último a los recopiladores.
	
	`Especifique la siguiente información para la transferencia de archivos:`
	`Host desde el que se importará el parche:`
	`Usuario en (nombre de host):`
	`Vía de acceso completo del parche, incluido el nombre (el nombre de archivo puede utilizar comodín *):`
	`(contraseña LDAP)Contraseña:`
	`Especifique el puerto SCP/FTP si necesita utilizar un puerto especial; de lo contrario, pulse Intro para continuar:`
	`El proceso de transferencia de archivo puede tardar un tiempo en completarse.`
	`Deje el terminal abierto y no responda ninguna pregunta hasta que se haya completado la transferencia.`
	`Iniciando la trasferencia, espere.`
	`La transferencia de archivo se ha completado.`
	`El perfil de copia de seguridad no está establecido para guardar el archivo de copia de seguridad cuando la instalación del parche ha fallado.`
	`Si desea guardar el archivo de copia de seguridad, responda NO a la pregunta y ejecute el mandato de CLI store backup profile para configurar los parámetros.`
	`¿Desea continuar (sí o no)? sí`
	`Liste los archivos en el directorio de parches:`
	`1. (nombre de archivo)`
	`Elija los parches que se instalarán (1-1, o varios números separados por ",", o q para salir): 1`
	`Instale el elemento 1`
	`El parche se ha enviado y se instalará según la hora de solicitud, compruebe el informe de parches instalados o la CLI (show system patch installed).`
	`No olvide eliminar el soporte, si es necesario.`

cd	La opción cd es para utilizarla en la instalación del parche desde un disco DVD. Para visualizar una lista completa de parches aplicados, consulte el informe Parches instalados en el separador Supervisor de Guardium del portal del administrador. También hay un informe Parches disponibles en el mismo separador Supervisor de Guardium. Para instalar un parche desde un DVD, antes de ejecutar este mandato inserte el DVD en la unidad de DVD ROM de IBM Guardium. Se mostrará una lista de los parches contenidos en el DVD.

- Para suprimir una solicitud de instalación de parche, utilice el mandato de CLI `delete scheduled-patch`
- Los parches permanecen después de la instalación sólo en el Gestor central. Los archivos de parches de unidades gestionadas o autónomas se suprimen después de la instalación.
- Para visualizar los parches disponibles: `show system patch available`
- Para visualizar los parches ya instalados y los parches planificados para su instalación, con fecha/hora y el estado de instalación: `show system patch installed`
- Utilice el mandato `fileserver` para iniciar un servidor de archivos basado en HTTPS que se ejecuta en el dispositivo de Guardium. Este recurso está pensado para facilitar la tarea de subida de parches a la unidad, o de la descarga de información de depuración de la unidad. Cada vez que se inicia este

recurso, éste suprime los archivos del directorio en el que sube los parches.
Nota: Cualquier operación que genere un archivo al que accederá el servidor de archivos debe finalizar antes de que se inicie el servidor de archivos (de forma que el archivo esté disponible para el servidor de archivos).

a. Para iniciar el archivo, especifique el mandato del servidor de archivos: `fileserver`
b. Iniciando el servidor de archivos. Puede encontrarlo en https://(nombre de la unidad)
c. Pulse INTRO para detener el servidor de archivos.
d. Abra el servidor de archivos en una ventana del navegador y realice una de las acciones siguientes:
   - Para subir un parche, pulse Subir un parche y siga las indicaciones.
   - Para descargar datos de registro, pulse Registros Sqlguard, vaya al archivo que desee, pulse con el botón derecho del ratón sobre él y descárguelo tal como lo haría con cualquier otro archivo.
e. Cuando haya terminado, vuelva a la sesión de CLI y pulse **Intro** para terminar la sesión.

Utilice la interfaz de usuario para mover los parches del Gestor central a las unidades gestionadas

6. Pulse Configuración > Herramientas y vistas > Distribución de parches.

   El botón Distribución de parches abrirá una nueva pantalla, mostrará una lista de parches disponibles con dependencias y permitirá la selección de un parche e instalarlo en todas las unidades seleccionadas. La lista de parches disponibles se construye a partir de los parches disponibles y se evalúan los parches instalados actualmente en cada una de las unidades seleccionadas, junto con la lista de dependencias de los parches disponibles. Los parches disponibles pero no instalables (falta un parche dependiente) se muestran en la lista en gris y no se pueden seleccionar. La selección del parche para instalar es una única selección, sólo se puede instalar un parche cada vez. Una vez que se ha seleccionado un parche y se ha pulsado el botón Instalar, se envía un mandato a todas las unidades seleccionadas para instalar ese parche; este proceso de instalación de parche se realizará en segundo plano.

7. Vaya a Gestión central > Gestión central > Distribución de parches.
8. Pulse Estado de instalación de parches. La pantalla Estado de instalación de parches aparece para cada unidad, las situaciones de instalaciones fallidas y discrepancias como, por ejemplo, un parche que sólo se instala en parte de las unidades, independientemente de si ha fallado en otras unidades o si no se ha instalado.

Resultados

Los sistemas donde se ha aplicado los parches están listos para su uso, pero recuerde que después de instalar un parche debe reiniciar el sistema Guardium.

Tema principal: Gestión del sistema Guardium
Información relacionada:
Cómo descargar e instalar un parche de Guardium (vídeo)

Mantenimiento de soporte

La característica Mantenimiento de soporte está protegida con contraseña y sólo se puede utilizar tal como lo indique el soporte técnico. Si requiere información adicional, póngase en contacto con el Soporte técnico.

Tema principal: Gestión del sistema Guardium

Integración de productos

Puede integrar IBM Guardium con otros productos.

- Configurar BIG-IP Application Security Manager (ASM) para la comunicación con el sistema Guardium
  Utilice Big-IP ASM (de F5 Networks) junto con la supervisión de actividad de base de datos en tiempo real de Guardium para resolver el problema de propagación de identidad entre la capa de aplicación web y la capa de servidor de aplicaciones de base de datos.
- Integración de Hadoop
  En este tema se presentan los procesos y conceptos fundamentales para supervisar los datos de Hadoop con Guardium.
- Integración de PIM con Guardium DAM
  Privileged Information Management (PIM) ayuda a las organizaciones a automatizar y realizar el seguimiento del uso de identidades con privilegios compartidas y a supervisar el uso de estas identidades con privilegios compartidas.
- Integración de QRadar y Guardium
  QRadar y Guardium pueden funcionar juntos en un flujo de información bidireccional para que las políticas de protección de datos de Guardium se actualicen automáticamente y prácticamente en tiempo real en respuesta a sucesos de inteligencia de seguridad de QRadar.
- Interfaz de OPTIM a Guardium
  Una interfaz de OPTIM a Guardium, que utiliza Protobuf (Universal Feed Agent), envía registros de actividad de Optim a Guardium.
- Combinación de alertas en tiempo real y análisis de correlación con productos SIEM
  Distribuya el conocimiento contextual de los patrones, estructuras y protocolos de base de datos directamente a la base de datos de terceros del sistema SIEM.
- Cómo transferir datos confidenciales a InfoSphere Discovery
  Tome información de datos confidenciales, identificados y clasificados en IBM Security Guardium y transfiera esta información a InfoSphere Discovery.
- Correlación con CEF
  El estándar CEF de ArcSight define un conjunto de campos necesarios y un conjunto de campos opcionales.
- Correlación LEEF
  Log Event Extended Format (LEEF) de QRadar

Configurar BIG-IP Application Security Manager (ASM) para la comunicación con el sistema Guardium

Utilice Big-IP ASM (de F5 Networks) junto con la supervisión de actividad de base de datos en tiempo real de Guardium para resolver el problema de propagación de identidad entre la capa de aplicación web y la capa de servidor de aplicaciones de base de datos.

Esta solución utiliza almacenamientos intermedios de protocolo de Google (.protobuf) como formato de conexión entre BIG-IP ASM y el sistema Guardium.

La información sobre la configuración de la integración entre Big-IP ASM y la supervisión de actividad de base de datos en tiempo real de Guardium se proporciona en el sitio web de F5: http://www.f5.com/pdf/deployment-guides/ibm-guardium-asm-dg.pdf.

Tema principal: Integración de productos

Integración de Hadoop

En este tema se presentan los procesos y conceptos fundamentales para supervisar los datos de Hadoop con Guardium.

Planificación de capacidad

Las siguientes directrices de dimensionamiento presuponen un volumen medio de tráfico auditado. Es posible que volúmenes más altos de tráfico auditado requieran recursos adicionales.

- 10 nodos de servidor o de gestión por recopilador
- 20 o más nodos de datos por recopilador, donde se necesitan S-TAP para los nodos de datos (los S-TAP no son necesarios para todos los componentes)
- Posiblemente nodos adicionales por recopilador si se utilizan dispositivos físicos

También es posible dimensionar por la unidad de valor de procesador (PVU) de los nodos, pero esto puede dar como resultado un tamaño excesivo si se auditan volúmenes de tráfico bajos. La directriz de dimensionamiento de capacidad es de 4000 PVU por recopilador.

Escenarios de integración

Si utiliza cifrado SSL con Cloudera, consulte Integración de Hadoop utilizando Cloudera Navigator.

Si utiliza cifrado SSL con un clúster Hadoop de Hortonworks, consulte Integración de Hadoop utilizando Hortonworks y Apache Ranger.
Nota: No se da soporte a la redacción de datos devueltos utilizando Hive. Si requiere la redacción de datos con Hive, consulte Integración de Hadoop utilizando un S-TAP estándar de Guardium.

Si no requiere cifrado SSL para el clúster de Hadoop, consulte Integración de Hadoop utilizando un S-TAP estándar de Guardium.

- Integración de Hadoop utilizando un S-TAP estándar de Guardium
  Obtenga información sobre cómo integrar Hadoop utilizando un S-TAP estándar de Guardium para HDFS y la supervisión de MapReduce.
- Integración de Hadoop utilizando Cloudera Navigator
  Obtenga información sobre cómo integrar Haddop utilizando Cloudera Navigator, la solución de gobierno de datos nativa de Cloudera.
- Integración de Hadoop utilizando Hortonworks y Apache Ranger
  Apache Ranger, incluido con Hortonworks Data Platform, ofrece control de acceso detallado y auditoría sobre componentes de Hadoop como Hive, HBASE y HDFS utilizando políticas.

Tema principal: Integración de productos
Información relacionada:
Parámetros de configuración de S-TAP para Hadoop

Integración de Hadoop utilizando un S-TAP estándar de Guardium

Obtenga información sobre cómo integrar Hadoop utilizando un S-TAP estándar de Guardium para HDFS y la supervisión de MapReduce.

Los despliegues de Hadoop incluyen dos componentes fundamentales:

- Hadoop Distributed File System (HDFS), que almacena datos
- MapReduce o MapReduce 2), que proporciona una infraestructura para acceder a los datos y analizarlos

La captura de actividad en estos dos componentes cubre los requisitos de auditoría básicos porque todos los datos, excepto el tráfico de la consola de gestión, pasan a través de HDFS.

Tenga en cuenta que la actividad de HDFS no es compatible con el auditor, ya que es similar a la supervisión del acceso a archivos en una base de datos relacional. Considere la posibilidad de supervisar la actividad de otros componentes utilizados en el entorno, como por ejemplo Hive, Big SQL o Impala. Estos componentes dan soporte a la supervisión que más se asemeja a los accesos a base de datos.

Políticas de bloqueo y redacción

Guardium da soporte a la redacción utilizando reglas de extrusión y al bloqueo mediante S-GATE Terminate para Hive e Impala. El bloqueo para BigSQL estaba soportado en la versión 9.x cuando se utiliza el S-TAP.

Para ver instrucciones detalladas sobre cómo utilizar las políticas de bloqueo y redacción con Hadoop, consulte IBM Security Guardium Deployment Guide for Hadoop Systems.

Kerberos

Guardium da soporte a la utilización de clústeres seguros de Kerberos con algunas restricciones. Para poder descifrar los ID de usuario de Kerberos, Guardium requiere que los archivos de tabla de claves se generen y se colocan en una ubicación específica. Hay disponibles instrucciones detalladas en IBM Security Guardium Deployment Guide for Hadoop Systems.

Atención: Es posible que la configuración de Kerberos sólo sea necesaria si utiliza HBase o Hive.

- Recomendaciones y limitaciones
  Debe seguir varias recomendaciones como guía para su integración de Guardium y Hadoop.
- S-TAP y motores de inspección con Hadoop
  Despliegue S-TAP de Guardium y configure los motores de inspección para su uso con Hadoop.
- Políticas y reglas de Guardium con Hadoop
  Empiece a crear políticas y reglas de Guardium para la supervisión de la actividad de Hadoop.
- Informes de Guardium con Hadoop
  Utilice los informes incorporados de Guardium para Hadoop o defina informes personalizados utilizando mandatos y objetos de Hadoop.

Tema principal: Integración de Hadoop

Recomendaciones y limitaciones

Debe seguir varias recomendaciones como guía para su integración de Guardium y Hadoop.

Recomendaciones para el despliegue

Para evitar inundar el recopilador y simplificar el diagnóstico de problemas, tenga en cuenta las tácticas siguientes para reducir la cantidad y los tipos de tráfico procesados por el recopilador de Guardium:

- Para limitar los datos que deben fluir a través de la red al dispositivo, restrinja el número de motores de inspección que configure.
- Para limitar la cantidad de datos que se registran en el recopilador, ponga condiciones en la política.

Una estrategia puede ser configurar y probar con las consultas de línea de mandatos de Hive antes de añadir motores de inspección adicionales y abrir la política para tráfico adicional de gran volumen como, por ejemplo, HDFS.

Para cada nuevo motor de inspección que configure, debe reiniciar S-TAP.

Recuerde que debe supervisar el sistema Guardium a medida que más servicios generen tráfico. El Redbook de despliegue de Guardium incluye información sobre cómo supervisar el sistema y asegurarse de que el tráfico no es excesivo para el recopilador.

Limitaciones

Se aplican las restricciones siguientes al supervisar Hadoop con un S-TAP estándar de Guardium:

- El cifrado SSL no está soportado a menos que se utilice Hortonworks con Ranger o Cloudera con Cloudera Manager. La integración de Ranger y Cloudera Manager se trata en una sección aparte de esta información.
- No se da soporte al encadenamiento de UID.
- Sólo se da soporte al bloqueo y la redacción para Big SQL, Hive e Impala.
- Actualmente se da soporte al sistema de auditoría de configuración y al descubrimiento de datos confidenciales.
- Actualmente Guardium no da soporte a la auditoría de mandatos de administración, por ejemplo, el inicio y la detención de servicios.
- Las opciones de equilibrio de carga y sustitución por anomalía de Guardium no están soportadas cuando se utiliza Kerberos, pero una opción puede ser utilizar F5 y otro equilibrio de carga en el que se utilice una dirección IP virtual.

Consideraciones sobre IBM InfoSphere BigInsights y Big SQL

A diferencia de la mayoría de las otras distribuciones de Hadoop, se aplican las siguientes restricciones a Hadoop en GPFS y Big SQL.

Hadoop en PGFS (IBM Spectrum Scale)
: El despliegue GPFS de BigInsights requiere el conector de transparencia de HDFS.

Big SQL
: Debe haber instalado un S-TAP en todos los nodos en los que haya instalado un motor de Big SQL. El soporte de Big SQL es completo y similar a lo que ya soporta Guardium para DB2.

  Si se utiliza Kerberos o GPFS, debe configurar una salida de comunicaciones especial en cada nodo de Big SQL. Guardium proporciona una biblioteca compartida cargada dinámicamente que interactúa con Big SQL, y Big SQL invocará funciones dentro de esa biblioteca en el tiempo de ejecución cuando realiza solicitudes de SQL y de programa de utilidad.
  Restricción: Sólo se da soporte a la supervisión y la auditoría utilizando la metodología de salida con Big SQL: la redacción y el bloqueo son características avanzadas que sólo están soportadas utilizando un S-TAP.

Tema principal: Integración de Hadoop utilizando un S-TAP estándar de Guardium

S-TAP y motores de inspección con Hadoop

Despliegue S-TAP de Guardium y configure los motores de inspección para su uso con Hadoop.

Despliegue de S-TAP y clientes GIM

Sólo se requieren S-TAP y clientes GIM puesto que Guardium aún no da soporte a CAS ni a descubrimiento de base de datos para Hadoop. Como con cualquier despliegue de S-TAP, asegúrese de descargar el S-TAP correcto para su sistema operativo y nivel de kernel.

Atención: Se recomienda un S-TAP para los nodos de límite, especialmente si los utiliza como una zona de destino de datos.

Configuración de motores de inspección

Una vez que se hayan desplegado los S-TAP, se deben definir los motores de inspección adecuados desde el dispositivo de Guardium. Los motores de inspección especifican el tráfico que se supervisa desde un host S-TAP determinado. Por ejemplo, en un host S-TAP determinado, un motor de inspección podría indicar que Guardium debe supervisar tráfico de los puertos 8032 y 60000. Los motores de inspección también especifican el protocolo a supervisar como, por ejemplo, Hadoop o HTTP.

Antes de configurar los motores de inspección, trabaje con el administrador de Hadoop para recopilar la siguiente información para cada nodo de Hadoop que se deba supervisar:

- nodo y servicio de Hadoop que se supervisarán
- números de puerto para los servicios
- dirección IP del servidor (es decir, dirección IP del host S-TAP)

Determine el protocolo del motor de inspección según el tipo de nodo y el servicio de Hadoop tal como se indica en la tabla siguiente.

Tabla 1. Protocolos del motor de inspección para nodos y servicios de Hadoop.

Nodo Hadoop	Servicio Hadoop	Protocolo del motor de inspección
Namenode	Nombre de nodo HDFS	Hadoop
Namenode	Puerto HTTP para WebHDFS	WEBHDFS
Namenode	Gestor de recursos para YARN	Hadoop
Rastreador de trabajos Nota: Este nodo sólo se requiere para MapReduce1.	Rastreador de trabajos de MapReduce	Hadoop
HBase maestro	HBase maestro	Hadoop
Región de HBase	Región de HBase	Hadoop
hiveserver2	Mensajes de protocolo Thrift	HIVE
Hive Metastore	Mensajes de protocolo Thrift, utilizados para obtener el usuario de base de datos Impala e Hive de Hue. Nota: Requiere la utilización de un atributo calculado.	HADOOP
Daemons Impala	Impala	IMPALA
Impala	Impala desde Hue	HIVE Nota: Impala desde Hue utiliza hiveserver2.
Nodo de gestión	Servidor BigSQL	DB2
Nodo de cálculo	Servidor BiGSQL	DB2
Nodo Hue	Interfaz de usuario de Hue con programa de fondo Oracle, MySQL o PGSQL	HUE
Nodo de búsqueda Solr	Búsqueda de Solr	HTTP

Por ejemplo, un nodo de nombre de HDFS puede utilizar el puerto `8020`, el protocolo `Hadoop` y tener una dirección de host de `10.0.0.21`.
Dada esta información, para configurar un motor de inspección, vaya a Gestionar > Actividad > Supervisión > Control de S-TAP en la interfaz de usuario de Guardium o utilizando mandatos de API de Guardium. Un ejemplo de mandato de API de Guardium puede ser similar al siguiente:

```
grdapi create_stap_inspection_engine client=0.0.0.0/0.0.0.0 protocol=HADOOP
    ktapDbPort=8020 portMax=8020 portMin=8020 connectToIp=127.0.0.0 stapHost=10.0.0.21
```

Restricciones:

- La CLI Hive está en desuso en distribuciones Hadoop y no está soportada en Guardium.
- Impala requiere configurar motores de inspección para todos los nodos que ejecutan un daemon de Impala.
- HBase requiere S-TAP en todos los nodos de datos, incluido el nodo maestro.
- Si utiliza Big SQL con Kerberos o GPFS, debe configurar el S-TAP con DB2_Exit, que es una manera segura y eficiente de capturar tráfico cifrado de Big SQL/DB2 y/o GPFS. Sin embargo, el bloqueo y la redacción no están soportados en este escenario. Encontrará información adicional sobre el soporte Big SQL en IBM developerWorks para Guardium.

Encontrará ejemplos adicionales e instrucciones más detalladas en IBM Security Guardium Deployment Guide for Hadoop Systems.
Tema principal: Integración de Hadoop utilizando un S-TAP estándar de Guardium

Políticas y reglas de Guardium con Hadoop

Empiece a crear políticas y reglas de Guardium para la supervisión de la actividad de Hadoop.

A efectos de supervisión, es útil pensar en términos del usuario, del objeto de datos que se está supervisando y las acciones o de los mandatos que se ejecutan. En terminología de Guardium, estos son el *Usuario de base de datos*, el *objeto* y el *verbo* o *mandato*, respectivamente. Estas entidades se pueden utilizar en reglas de política para desencadenar acciones determinadas, como las alertas en tiempo real.

Las acciones de reglas de política de Guardium le permiten filtrar el tráfico por motivos de rendimiento, además del registro y las alertas sobre infracciones políticas. Para el tráfico de Hadoop, no puede utilizar acciones de filtrado a nivel de sesión como, por ejemplo, *ignorar sesión S-TAP*. Esto se debe a que Hadoop no realiza la gestión de sesiones de la misma manera que las bases de datos relacionales en las que se inicia la sesión en la base de datos, que establece una sesión y, a continuación, genera el tráfico de SQL antes de finalizar la sesión. Con Hadoop, cada mandato es su propia sesión y puede generar muchas más sesiones a medida que el trabajo se distribuye por todo el clúster.

Guardium no puede normalmente detectar inicios de sesión fallidos para componentes de línea de mandatos, aunque Guardium puede ver inicios de sesión fallidos desde Hue y a través de IBM BigSQL.

Obtendrá excepciones de permiso a nivel de sistema de archivos, de modo que informará sobre los que utilicen el dominio de excepciones.

Empiece a crear políticas desde la política incorporada de Hadoop para garantizar que se captura el tráfico. Se recomienda que pruebe la política predeterminada en un entorno de prueba de tráfico bajo, e incluso puede añadir una o más reglas de acceso para restringir el tráfico a un único tipo de servidor, como por ejemplo Hive, a fin de reducir la cantidad de ruido que ve. Una vez que esté seguro de que el tráfico fluye hacia el recopilador, puede clonar la política predeterminada y crear una que se alinee con sus requisitos de cumplimiento y seguridad.

Para obtener instrucciones detalladas y un ejemplo de políticas para un entorno Hadoop de producción, consulte la publicación IBM Security Guardium Deployment Guide for Hadoop Systems.

Tema principal: Integración de Hadoop utilizando un S-TAP estándar de Guardium

Informes de Guardium con Hadoop

Utilice los informes incorporados de Guardium para Hadoop o defina informes personalizados utilizando mandatos y objetos de Hadoop.

Guardium incluye varios informes incorporados para Hadoop. Para ver la lista de informes disponibles, vaya a Mis paneles de control > Crear un nuevo panel de instrumentosy pulse Añadir informe. En la ventana Añadir un informe, escriba `hadoop` en el campo de búsqueda para ver una lista de informes de Hadoop disponibles.

Algunos de los informes incorporados proporcionan informes basados en componentes, que son útiles cuando se valida la configuración y que se está capturando correctamente el tráfico del componente. Otros informes se centran más en la seguridad y el cumplimiento, como por ejemplo *Hadoop - Informe de permisos*, *Hadoop - Usuarios privilegiados que acceden a objetos confidenciales*, *Hadoop -Informe de excepción* y *Hadoop - Inicio de sesión del usuario*.

En esta sección se incluyen listas de objetos y mandatos o verbos utilizados con Hadoop. Puede cortar y pegar los mandatos en un grupo de Guardium utilizando la herramienta Creador de grupos. También deberá grupos de usuarios y objetos basados en su propio entorno.

Objetos de Hadoop

- Archivos/directorios HDFS
- Nombre de trabajo de MapReduce 2

  Antes de MapReduce 2, el nombre de trabajo de MapReduce no se registraba como un objeto separado, pero se podía obtener utilizando el informe MapReduce incorporado y sus atributos calculados para obtener el nombre de trabajo del mensaje completo.
- Nombre de vista y tabla de IBM Big SQL, Impala, Hive, HBase

Mandatos de HDFS

Mandatos de lectura de HDFS:

- getFileInfo
- getBlockLocations
- getFileLocation
- getListing

Mandatos de grabación de HDFS:

- addBlock
- complete
- create
- delete
- mkdirs
- rename

Mandatos de HBase

Mandatos de lectura de HBase:

- list
- scan

Mandatos de grabación de HBase:

- createTable
- disableTable
- deleteTable
- multi

  Normalmente, es un mandato insert/update. Con la opción de despliegue de integración de Ranger, es un mandato put.
- drop

Objetos y mandatos de Big SQL, Hive e Impala

Los lenguajes de consulta de Big SQL, Hive e Impala son como SQL y dan soporte a las reglas normales de análisis y registro utilizadas con la mayoría de las otras bases de datos relacionales de Guardium. Muchos de estos mandatos ya están incluidos en los grupos de mandatos de Guardium, por ejemplo, los mandatos ALTER, los mandatos CREATE y los mandatos administrativos. La extensión del soporte de la sintaxis de SQL varía mucho entre estas distribuciones, entre las que Big SQL tiene el soporte más amplio.

Tema principal: Integración de Hadoop utilizando un S-TAP estándar de Guardium

Integración de Hadoop utilizando Cloudera Navigator

Obtenga información sobre cómo integrar Haddop utilizando Cloudera Navigator, la solución de gobierno de datos nativa de Cloudera.

Guardium da soporte a la auditoría para Cloudera Hadoop utilizando un S-TAP estándar. Para obtener más información, consulte Integración de Hadoop utilizando un S-TAP estándar de Guardium.

Guardium también proporciona la capacidad de suscribirse a sucesos de auditoría cuando Cloudera Navigator está configurado con Kafka como un destino de registro alternativo. La actividad auditada se envía a un clúster de Kafka donde el S-TAP de Guardium consume los sucesos y los envía al dispositivo recopilador de Guardium para su análisis y registro. Una vez que los datos están en Guardium, están altamente protegidos y se pueden utilizar todas las funciones normales de Guardium como por ejemplo la creación de alertas en tiempo real y la integración con SIEM, la creación de informes y el flujo de trabajo, y el análisis.

Comparado con la integración utilizando un S-TAP estándar de Guardium, la integración con Cloudera Navigator da soporte al cifrado SSL para los clientes que acceden a los datos de Hadoop. Cuando se utiliza la integración con Cloudera Navigator, los datos se descifran antes de que el dispositivo de Guardium los reciba.

Restricción: El bloqueo basado en Guardium no está soportado para los componentes de Hadoop cuando se utiliza la integración con Cloudera Navigator.

Requisitos previos

La integración de Guardium con Cloudera Navigator requiere los siguientes niveles mínimos de release de software:

- IBM Security Guardium y S-TAP V10.1.2 o posterior
- CDH 5.7, Cloudera Manager 5.8 y la versión de Kafka incluida con estos releases

Arquitectura y flujo de datos

En lugar de tener un S-TAP que resida en los servidores Hadoop, el agente de Cloudera Manager envía sucesos de auditoría desde los registros de componentes de Hadoop al servidor de auditoría de Cloudera Navigator. En este punto, Cloudera Navigator graba los sucesos de auditoría en su base de datos de auditoría. Para integrarlo con Guardium, establezca Kafka como un registrador adicional: Guardium recopilará los registros de sucesos de Kafka.

La configuración es bastante flexible ya que puede instalar el S-TAP en un nodo en el clúster de Hadoop o en un servidor separado fuera del clúster de Hadoop, siempre que dicho servidor tenga conectividad de red con el clúster de Kafka y el dispositivo de Guardium. Sólo puede especificar un S-TAP por clúster de Kafka, pero ese S-TAP puede enviar tráfico a varios sistemas Guardium utilizando técnicas estándar de alta disponibilidad o de equilibrio de carga.

En esta configuración, Cloudera Navigator genera los sucesos de registro para cada componente de Hadoop, y el S-TAP consume estos sucesos. Mediante la interfaz de usuario de Guardium, especificará el identificador de tema de mensaje que utiliza Cloudera Navigator para que el S-TAP de Guardium sepa qué sucesos se supone que debe tomar.

Recomendación: Utilice un clúster de Kafka seguro para asegurarse de que los sucesos de auditoría están protegidos.

- Planificación de la integración con Cloudera Navigator
  Complete y verifique las tareas de este tema antes de configurar la integración.

Tema principal: Integración de Hadoop
Información relacionada:
Parámetros de configuración de S-TAP para Hadoop

Planificación de la integración con Cloudera Navigator

Complete y verifique las tareas de este tema antes de configurar la integración.

La integración con Cloudera Navigator requiere recopilar información de los administradores responsables de Cloudera y Kafka, así como del equipo de seguridad de datos responsable de Guardium. Recopile la siguiente información antes de empezar:

- Host y puertos de los servidores de programa de arranque de Kafka
- Si se utiliza TLS y Kerberos en el clúster de Kafka.
- El host y el puerto del servidor donde está instalado el S-TAP. Verifique que haya conectividad de red entre este servidor y el clúster de Kafka y el sistema Guardium.
- El sistema operativo y la versión que utiliza el host S-TAP para que pueda descargar e instalar el S-TAP correcto.
- El host del sistema Guardium. Esto es necesario para instalar y configurar el S-TAP.

1. Configurar la solución para la supervisión
   En esta sección se describe cómo configurar la solución para la supervisión.
2. Configurar la comunicación entre Guardium y Cloudera Navigator
   Obtenga información sobre cómo establecer la comunicación entre el sistema Guardium y Cloudera Navigator utilizando un clúster de Kafka.

Tema principal: Integración de Hadoop utilizando Cloudera Navigator

Configurar la solución para la supervisión

En esta sección se describe cómo configurar la solución para la supervisión.

Procedimiento

1. Configure el componente de auditoría de Cloudera Navigator.

   Para obtener más información, consulte la documentación de Cloudera e Integración de IBM Security Guardium Activity Monitoring for Cloudera Hadoop utilizando Navigator.

2. Asegúrese de que TLS/SSL está configurado correctamente para Kafka.

   El clúster Kafka que utiliza para generar sucesos de auditoría de Cloudera no debe estar configurado para requerir la autenticación de cliente SSL. Para obtener más información, consulte Integración de IBM Security Guardium Activity Monitoring for Cloudera Hadoop utilizando Navigator.

3. Instale el S-TAP de Guardium en un servidor.

   Utilice cualquier método disponible para instalar el S-TAP en el servidor designado dentro o fuera del clúster de Hadoop. En Guardium, vaya a Gestionar > Vista del sistema > Supervisor de estado de S-TAPr para verificar la conectividad entre el S-TAP y el sistema Guardium.

   Para consultar los parámetros de configuración de S-TAP relacionados con Hadoop, consulte Parámetros de configuración de S-TAP para Hadoop.

4. Configure la publicación de los sucesos de auditoría de Cloudera Navigator en Kafka.

   El administrador de Navigator o el administrador completo deben realizar esta tarea desde Cloudera Manager. Para obtener más información, consulte Integración de IBM Security Guardium Activity Monitoring for Cloudera Hadoop utilizando Navigator.

5. Configurar la comunicación entre Guardium y Cloudera Navigator
6. Valide la configuración.

Después de configurar la solución, vuelva a Gestionar > Vista de sistema > Supervisor de estado de S-TAP y verifique que el estado de S-TAP aún sea verde. La verificación del motor de inspección no está soportada para los orígenes de Hadoop y siempre indicará un estado *No verificado*.

7. Instale las políticas de Guardium y Cloudera Navigator.

   Para la supervisión y auditoría, prácticamente no hay ninguna diferencia en las reglas de política entre cuando se utiliza la integración con Cloudera Navigator y cuando se utiliza la supervisión normal de S-TAP para Hadoop. Para empezar, instale una política de Guardium o utilice la política predeterminada, ejecute los mandatos HDFS o Hive en el clúster de Cloudera y verifique que puede ver el tráfico en un informe de Guardium. Para obtener más información, consulte Integración de IBM Security Guardium Activity Monitoring for Cloudera Hadoop utilizando Navigator.

Tema principal: Planificación de la integración con Cloudera Navigator
Tema siguiente: Configurar la comunicación entre Guardium y Cloudera Navigator

Configurar la comunicación entre Guardium y Cloudera Navigator

Obtenga información sobre cómo establecer la comunicación entre el sistema Guardium y Cloudera Navigator utilizando un clúster de Kafka.

Acerca de esta tarea

Vaya a **Configuración > Herramienta y vistas > Supervisión de Hadoop** y, a continuación, seleccione el icono más en el área **Añadir información de clúster**.

Procedimiento

1. Vaya a Configuración > Herramientas y vistas > Supervisión de Hadoopy pulse el icono más en el área Añadir información de clúster.
2. Utilice el menú Nombre de host S-TAPx para seleccionar un S-TAP que esté conectado al sistema Guardium.
3. Proporcione un Nombre de tema para el clúster de Kafka.

   A menos que esto se haya cambiado en los valores de configuración de clúster de Kafka, utilice `NavigatorAuditEvents` (valor predeterminado).

4. Utilice la sección Servidores de programa de arranque para especificar uno o más nodos de Kafka para realizar la conexión inicial desde el S-TAP de Guardium.

   Los nodos que sean líderes de una partición para el tema manejarán las solicitudes de los consumidores. Para las conexiones iniciales, es mejor especificar más de un servidor para proporcionar una sustitución por anomalía en caso de que uno de los servidores de programa de arranque esté inactivo.

5. Si el clúster de Kafka está configurado con TLS, marque el recuadro de selección Habilitar TLS.
   Restricción: Guardium no permite que los clústeres de Kafka configurados requieran autenticación de cliente SSL.
6. Si el clúster de Kafka requiere autenticación de Kerberos, marque el recuadro de selección Utilizar Kerberos.
   a. Utilice el campo Principal para proporcionar el nombre de principal de Kerberos para el S-TAP.

      Por ejemplo, `guardium/FullyQualifiedDomainName@kerberosDomain`.

   b. En el campo Vía de acceso de archivo de tabla de claves, proporcione la vía de acceso completa al archivo de tabla de claves de Kerberos en el servidor S-TAP.

      Por ejemplo, `/etc/krb.keytab`. Asegúrese de que la tabla de claves sea propiedad del usuario y grupo del S-TAP y de que sólo la pueda leer el usuario.

7. Pulse Guardar.

   El área resultante mostrará que ha configurado la supervisión de Hadoop y el estado de S-TAP debería ser verde.

Tema principal: Planificación de la integración con Cloudera Navigator
Tema anterior: Configurar la solución para la supervisión

Integración de Hadoop utilizando Hortonworks y Apache Ranger

Apache Ranger, incluido con Hortonworks Data Platform, ofrece control de acceso detallado y auditoría sobre componentes de Hadoop como Hive, HBASE y HDFS utilizando políticas.

Los datos de auditoría se graban en HDFS y en Solr (recomendado). Guardium se puede integrar con Ranger de dos formas:

- Para la auditoría, Guardium actúa como otra fuente de registrador para la auditoría de Ranger. La actividad auditada se envía al recopilador de Guardium, donde se analiza y se registra. Una vez que los datos están en Guardium, están altamente protegidos en el dispositivo reforzado, y se pueden utilizar todas las funciones normales de Guardium como por ejemplo la creación de alertas en tiempo real y la integración con SIEM, la creación de informes y el flujo de trabajo, y el análisis.
- Para el bloqueo, Guardium amplía las políticas de control de acceso de Ranger, utilizando lo que se conoce en Ranger como políticas dinámicas.

A diferencia de las integraciones de Hadoop que se basan en un S-TAP estándar de Guardium para la supervisión y el bloqueo, la integración con Ranger da soporte al cifrado SSL entre los datos de Hadoop y los clientes. Con la integración de Ranger, los datos se descifran antes de que se envíen al sistema Guardium para la auditoría. Además del soporte SSL, la integración de Ranger mediante políticas dinámicas habilita el soporte de bloqueo para más componentes de los soportados mediante el S-TAP estándar.

Aunque puede utilizar los motores de inspección y la integración de Ranger en el mismo clúster, es poco probable que se utilicen ambos métodos simultáneamente. Consulte Integración de Hadoop para obtener más información sobre cómo seleccionar un método de integración.

Requisitos previos

La integración con Ranger requiere lo siguiente:

- IBM Security Guardium 10.1 (S-TAP y dispositivo)
- Hortonworks 2.3 con Ranger

Arquitectura y flujo de datos

La diferencia importante con esta arquitectura es que el S-TAP no recopila datos de auditoría directamente del componente Hadoop; en lugar de ello, son los plugins de Ranger que están grabando los mensajes de auditoría en log4j, que los reenvían a S-TAP, los que a continuación envían los mensajes al recopilador de Guardium para el registro, las alertas, los informes y los análisis.

Debe configurar el S-TAP, especificando log4j_reader_enabled= 1, para activar la integración con Ranger.

La configuración es bastante flexible, ya que puede instalar los S-TAP en más nodos. Puede configurar Ranger para enviar todo el tráfico de componentes a un único S-TAP o puede especificar, por ejemplo, que todo el tráfico de HBase vaya a un S-TAP y que Hive y HDFS vayan a otro.

El bloqueo se implementa ampliando las políticas de control de acceso de Ranger para cumplir las reglas de política de bloqueo especificadas en el dispositivo de Guardium. La implementación real del bloqueo se lleva a cabo como una denegación de acceso de Ranger. Para obtener más información sobre cómo encaja el bloqueo en la arquitectura y el flujo de datos y las directrices para implementar el bloqueo, consulte Integración de la seguridad y el bloqueo de IBM Security para Hortonworks Hadoop utilizando Apache Ranger.

- Planificación de la integración con Hortonworks y Apache Ranger
  Complete y verifique las tareas de este tema antes de configurar la integración.
- Configurar la solución para la supervisión
  En esta sección se describe cómo configurar la solución para la supervisión.

Tema principal: Integración de Hadoop
Información relacionada:
Parámetros de configuración de S-TAP para Hadoop

Planificación de la integración con Hortonworks y Apache Ranger

Complete y verifique las tareas de este tema antes de configurar la integración.

Topología de los S-TAP y recopiladores

Determine la topología necesaria:

- Número de recopiladores necesarios
- Componentes supervisados por cada S-TAP

Algunos clientes prefieren tener un S-TAP para cada componente. Como mínimo, recomendamos un S-TAP para HBase y un S-TAP para todo lo demás.
Consejo: No es necesario que un S-TAP se coloque en el mismo nodo que un componente determinado. Es posible, e incluso recomendable si se da soporte a Hadoop HA, establecer un sistema Linux dedicado para un S-TAP.
Cuando configure el número de conexiones de un S-TAP, utilice la regla empírica siguiente:

- HBase: uno más el número de servidores de región
- Todo lo demás: uno más uno para cada componente supervisado

Atención:

- Para el bloqueo, verifique el acceso a todos los servidores de región de HBase, puesto que tendrá que copiar el archivo JAR del plugin de Guardium en cada uno de estos servidores de región.

  Para configurar escenarios de sustitución por anomalía de alta disponibilidad, registre los nombres de host o las direcciones IP del nodo de sustitución por anomalía.

Alta disponibilidad y sustitución por anomalía

Hadoop utiliza nodos secundarios para la alta disponibilidad para manejar las solicitudes de datos en caso de que falle el nodo primario. Tiene varias opciones para el despliegue de S-TAP para poder continuar recopilando datos de auditoría en un escenario de sustitución por anomalía.

Instale el S-TAP y configúrelo en un sistema que no forme parte del clúster de Hadoop
: Esto proporciona una configuración simple en la que, cuando se realiza la sustitución por anomalía de los componentes, el nuevo nodo utiliza automáticamente el S-TAP como un registrador remoto. No es necesario realizar ningún cambio en la configuración o S-TAP.

Utilice `localhost` para el S-TAP para HDFS e Hive y un sistema distinto para HBase
: Instale un S-TAP para HDFS e Hive utilizando `localhost` en el campo de host S-TAP y, a continuación, utilice un sistema aparte como, por ejemplo, un nodo de límite para HBase. Esto proporciona una alternativa a la instalación de S-TAP en todos los servidores de región y es el método recomendado.

Instalar el S-TAP en los nodos del clúster
: En este modelo, se instala un S-TAP en el nodo primario y en espera de cada componente.

  Utilizando `localhost` en el campo de host S-TAP, instale un S-TAP en cada nodo del clúster y en cada servidor de región para HBASE. No se recomienda este método.

Equilibrio de carga de Guardium

Cuando está habilitada la integración con Ranger se da soporte a las opciones de S-TAP de Guardium y equilibrio de carga empresarial.

Recopilar información de Ambari y Ranger

Una parte considerable de la configuración se realiza mediante Ambari, la interfaz administrativa de Hadoop. Para completar la configuración, necesitará la siguiente información:

Ambari

- Un ID de usuario y una contraseña que tenga privilegios para actualizar y guardar la configuración de *log4j*, como por ejemplo una cuenta de administrador de servicio. Por razones de simplicidad, los denominaremos la contraseña y la cuenta de administrador.
- Puerto y dirección IP o nombre de host.
- Nombre de clúster.

Ranger

La información siguiente sólo es necesaria si se configura el bloqueo. Para obtener más información sobre cómo configurar el bloqueo, consulte Integración de la seguridad y el bloqueo de IBM Security para Hortonworks Hadoop utilizando Apache Ranger.

- Una cuenta de administrador de servicios que pueda actualizar y guardar la configuración de *log4j*.
- Puerto y dirección IP o nombre de host.

Abrir los puertos necesarios

Asegúrese de que se han abierto los siguientes puertos (suponiendo el uso de los puertos predeterminados):

- Para la supervisión, abra el puerto 5555 entre el nodo o nodos en los que está el S-TAP y el servidor Ranger.
- Para el bloqueo, abra el puerto 5556 para permitir la comunicación entre S-TAP y todos los nodos del clúster que tienen el plugin de Guardium.

Tema principal: Integración de Hadoop utilizando Hortonworks y Apache Ranger

Configurar la solución para la supervisión

En esta sección se describe cómo configurar la solución para la supervisión.

Antes de empezar

Antes de empezar a configurar la comunicación de Guardium con Ranger, configure los plugins de Ranger mediante Ambari. Consulte la guía Integración de la seguridad y el bloqueo de IBM Security para Hortonworks Hadoop utilizando Apache Ranger o la documentación de Hortonworks para obtener más detalles.

1. Configurar la comunicación entre Guardium y Ranger
   Obtenga información sobre cómo establecer la comunicación entre el sistema Guardium y Ranger.
2. Instalar y configurar los S-TAP
   Instale y configure los S-TAP para la integración con Ranger.
3. Habilitar la supervisión para los servicios Hadoop
   Habilite la supervisión para componentes específicos de Hadoop.

Qué hacer a continuación

Una vez que haya completado estos pasos de configuración, instale las políticas de Guardium y Ranger. Para la supervisión y la auditoría, prácticamente no hay ninguna diferencia en las reglas de política entre cuando se utiliza Ranger y cuando se utiliza la supervisión estándar de S-TAP para Hadoop. Para obtener más información, consulte Integración de la seguridad y el bloqueo de IBM Security para Hortonworks Hadoop utilizando Apache Ranger.
Tema principal: Integración de Hadoop utilizando Hortonworks y Apache Ranger

Configurar la comunicación entre Guardium y Ranger

Obtenga información sobre cómo establecer la comunicación entre el sistema Guardium y Ranger.

Acerca de esta tarea

Esta tarea describe cómo establecer la comunicación entre el sistema Guardium y Ranger.

Procedimiento

1. Vaya a Configuración > Herramientas y vistas > Supervisión de Hadoop.
2. Pulse el en la sección Añadir información de clúster para empezar a definir una nueva configuración.
3. Utilice el campo Nombre para proporcionar un nombre para la configuración.
4. Seleccione `Hortonworks` en el menú Distribución de Hadoop.
5. En el campo IP/Nombre de host, proporcione el nombre de host o la dirección IP del servidor de Ambari.
6. En el campo Número de puerto, proporcione el número de puerto del servidor de Ambari. Si deja este campo en blanco, la configuración utilizará el puerto predeterminado de 8080.
7. En el campo Nombre de clúster, proporcione el nombre de clúster de Hadoop.
8. En el campo Nombre de usuario, proporcione un nombre de usuario de administrador de Ambari.
9. En el campo Contraseña, proporcione una contraseña para la cuenta de administrador de Ambari.
10. Pulse el botón Probar conexión para verificar la configuración.
11. Pulse Guardar para guardar la configuración.

Resultados

La nueva configuración estará disponible en la página Supervisión de Hadoop.
Tema principal: Configurar la solución para la supervisión
Tema siguiente: Instalar y configurar los S-TAP

Instalar y configurar los S-TAP

Instale y configure los S-TAP para la integración con Ranger.

Antes de empezar

Revise Planificación de la integración con Hortonworks y Apache Ranger para obtener información sobre los requisitos de los S-TAP y las opciones de despliegue.

Procedimiento

1. Instale los S-TAP y habilítelos para la integración con Ranger. Es posible que necesite más de un S-TAP para manejar el tráfico, por ejemplo, configurar un S-TAP en el nodo de nombre para el tráfico de HDFS, Hive y Kakka, y otro S-TAP en el nodo maestro de HBASE para todo el tráfico de HBase.
2. Configure guard_tap.ini para la auditoría.
   a. Abra guard_tap.ini en un editor de texto. Debe editar el archivo directamente, ya que no hay soporte de UI o GIM para estos valores.
   b. Añada los parámetros que se listan a continuación. Actualice los valores para que reflejen

```
; Settings for log4j
logging log4j_reader_enabled=1
log4j_port=5555
log4j_listen_address=0.0.0.0
; Maximum number of connections to support from the log4j service
log4j_num_connections=50
```

   c. Reinicie el S-TAP después de actualizar los valores.

Tema principal: Configurar la solución para la supervisión
Tema anterior: Configurar la comunicación entre Guardium y Ranger
Tema siguiente: Habilitar la supervisión para los servicios Hadoop
Información relacionada:
Parámetros de configuración de S-TAP para Hadoop

Habilitar la supervisión para los servicios Hadoop

Habilite la supervisión para componentes específicos de Hadoop.

Acerca de esta tarea

Esta tarea describe cómo definir qué componentes de Hadoop están habilitados para la supervisión con Guardium.

Procedimiento

1. Vaya a Configuración > Herramientas y vistas > Supervisión de Hadoop.
2. Para empezar a configurar los servicios, pulse el de un clúster de Hadoop.
3. Utilice el menú Servicio para seleccionar el componente Hadoop en el que desea habilitar la supervisión.
4. Utilice el menú Nombre/IP de host S-TAP para seleccionar el sistema S-TAP donde desea recopilar los sucesos de auditoría de Ranger.
5. En el campo Número de puerto, proporcione el número de puerto de escucha. Si deja este campo en blanco, el servicio utilizará el puerto predeterminado de 5555.
6. Seleccione Activar la supervisión inmediatamente para habilitar la supervisión para los servicios seleccionados.
7. Pulse el botón Guardar para guardar la configuración de servicios.
   Atención: El administrador de Hadoop debe reiniciar el servicio Hadoop para activar los cambios realizados en la configuración de los servicios.

Resultados

En la página Supervisión de Hadoop, verifique que los servicios habilitados están marcados con un icono de marca de selección verde.

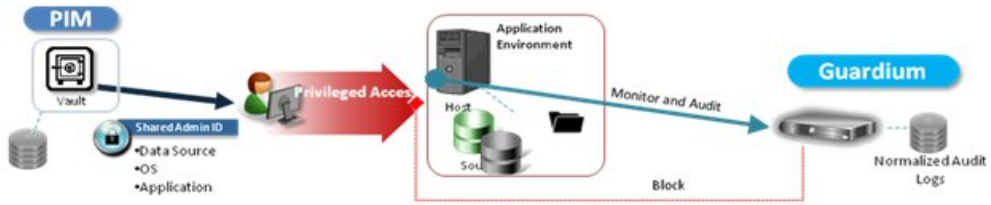
Tema principal: Configurar la solución para la supervisión
Tema anterior: Instalar y configurar los S-TAP

Integración de PIM con Guardium DAM

Privileged Information Management (PIM) ayuda a las organizaciones a automatizar y realizar el seguimiento del uso de identidades con privilegios compartidas y a supervisar el uso de estas identidades con privilegios compartidas.

La idea es integrar los datos de actividad de PIM con los datos de Guardium DAM, a fin de permitir la visibilidad al usuario real (la persona) que ha iniciado sesión en la base de datos.

El diagrama ilustra la integración.



El objetivo principal de esta integración es:

- Proporcionar visibilidad en los dispositivos de Guardium a los datos de PIM como, por ejemplo, el historial de alquiler (quién ha utilizado las cuentas compartidas), las credenciales y las bases de datos gestionadas por PIM.
- Proporcionar información de DAM correlacionada con la información de PIM, por ejemplo, Guardium puede mostrar el usuario de la base de datos de hoy junto con las solicitudes reales emitidas por un usuario específico. Esta integración permitirá el uso tanto del usuario de la base de datos como del usuario real de PIM que ha alquilado el ID compartido.

Instalación

Se puede utilizar el parche de Guardium (v10.1p103) para instalar la funcionalidad de integración de PIM. La integración de PIM se puede utilizar en sistemas Guardium autónomos así como en entornos federados.

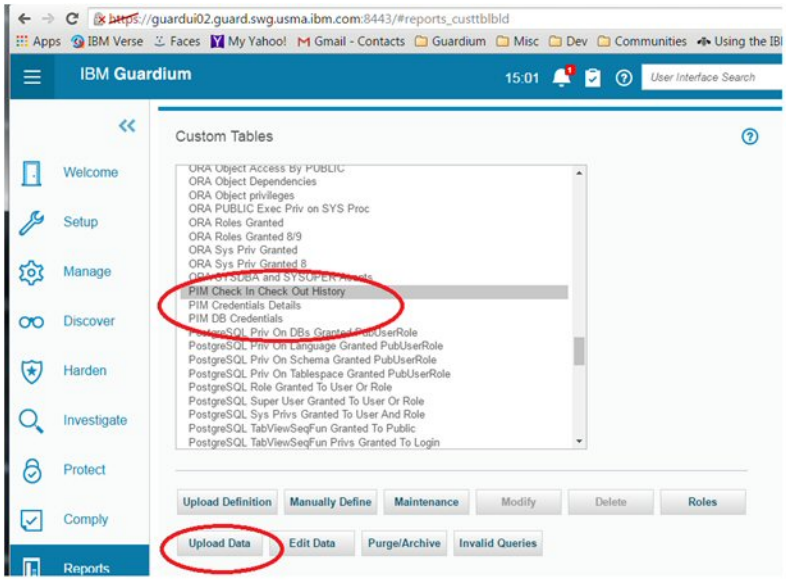
Nota: Se supone que los datos de actividad de PIM ya están implementados.

Siga estos pasos

1. Lleve los datos al sistema Guardium.

   Seleccione un origen de datos y, a continuación, selecciónese en la interfaz de usuario de Guardium: Informes > Herramienta de configuración de informes > Generador de tablas personalizadas.

   Localice y seleccione tres tablas predefinidas de PIM y, para cada una de ellas, planifique la subida automática de datos.



   Subir tablas de PIM a sistema Guardium

   Si utiliza un Gestor central de Guardium, seleccione en la interfaz de usuario de Guardium: Gestionar > Gestión central > Distribución de datos de PIM. Haga esto para planificar la distribución de datos desde el Gestor central a todas las unidades gestionadas.

2. Cuando haya llevado los datos a las unidades gestionadas, utilice este mandato de CLI, store pim_correlation_mode, para habilitar la correlación de datos de PIM con los datos de sesión de Guardium.

   Mandato de CLI

   store pim_correlation_mode

   Uso: store pim_correlation <estado>

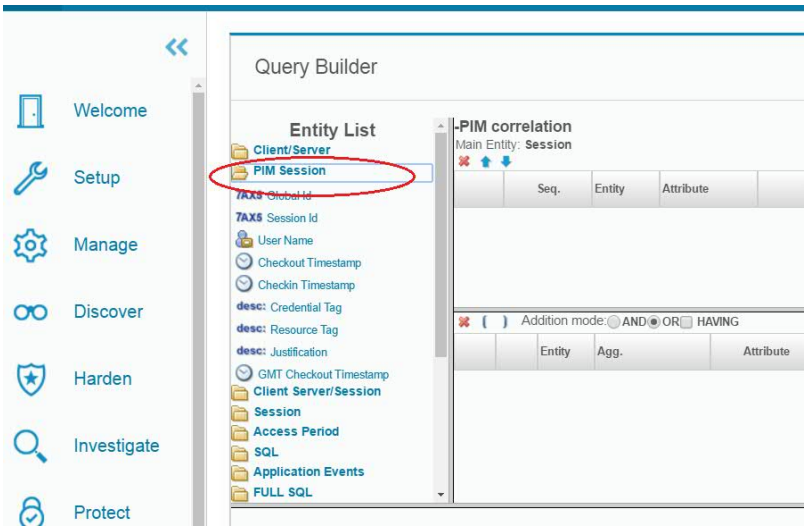
   donde estado es activado/desactivado. Activado es para habilitarla y Desactivado para inhabilitarla.

   Mandato Show

   show pim_correlation_mode

3. Para ejecutar la correlación, seleccione desde la interfaz gráfica de usuario de Guardium: Cumplir > Creación de informes personalizados > Correlación de datos de PIM.

   Los datos correlacionados se pueden ver mediante informes en el dominio Acceso



   Sesión de PIM en el dominio Acceso

Integración de QRadar y Guardium

QRadar y Guardium pueden funcionar juntos en un flujo de información bidireccional para que las políticas de protección de datos de Guardium se actualicen automáticamente y prácticamente en tiempo real en respuesta a sucesos de inteligencia de seguridad de QRadar.

IBM QRadar es una herramienta de inteligencia de seguridad que proporciona protección frente a amenazas mediante la supervisión de sucesos y la información de seguridad, utilizando reglas personalizables para detectar anomalías, así como proporcionando herramientas para la gestión de vulnerabilidades y el análisis forense de incidencias.

IBM Guardium es una solución para la seguridad y la privacidad de datos que ayuda a garantizar la integridad de los datos almacenados en los servidores. Guardium utiliza políticas y listas de inclusión/exclusión (denominadas grupos de Guardium) para controlar el acceso a los datos.

La solución de QRadar y Guardium aprovecha la infraestructura de QRTrigger para desencadenar acciones en respuesta a sucesos de seguridad de QRadar. En función de los valores de configuración, los sucesos de QRadar harán que se añadan nuevos miembros a los grupos de Guardium según la información que contiene el propio suceso. Además, la política de Guardium asociada con el grupo se reinstala automáticamente para que el cambio de pertenencia surta efecto inmediatamente.

Tenga en cuenta que la solución de QRadar y Guardium se puede utilizar para actualizar un único recopilador de Guardium o bien un grupo de ellos que controla un Gestor central de Guardium.

QRadar y Guardium juntos

La integración tradicional de QRadar y Guardium es un flujo de información unidireccional donde Guardium envía informes de alertas y asesoramiento de vulnerabilidades (VA) a QRadar.

Casos de uso de alertas comunes para bases de datos:

- Inicios de sesión fallidos
- Acceso no autorizado
- Códigos de error de SQL (por ejemplo, ataques de inyección SQL)
- Usuarios que intentan escalar sus privilegios
- Usuarios que crean desencadenantes y vistas para acceder de forma indirecta a datos confidenciales

Ahora QRadar y Guardium pueden trabajar juntos en un flujo de información bidireccional.

Casos de uso adicionales:

- Bloquear el acceso desde una máquina que se ha comprometido
- Aumentar los niveles de auditoría para el acceso con un ID de usuario que ahora es sospechoso
- Aumentar los niveles de auditoría para el acceso con un ID de usuario compartido con privilegios que se ha incorporado en un sistema PIM (gestión de identidades con privilegios)

Actualización de políticas de Guardium basadas en sucesos de QRadar

Los pasos para desplegar la solución QRadar y Guardium son:

1. Instale los archivos de solución.
2. Configure un ID y secreto de cliente en Guardium.
3. Configure un destino de reenvío en QRadar.
4. Configure reglas para enviar sucesos de QRadar a la solución.
5. Si es necesario, defina Políticas y grupos de Guardium para la integración.

Tenga en cuenta que Guardium versión 10.1 y posterior tiene tres grupos predefinidos diseñados para dar soporte a esta integración:

- QRadarBlockingConnection
- QRadarAlertingConnection
- QRadarLogConnection

Cada uno de estos grupos tiene la estructura de tupla siguiente:

<IP de cliente>,<Aplic. origen>,<Usuario de BD>,<IP de servidor>,<Nombre serv.>,<Usuario de SO>,<Nombre de BD>

Existe una política de Guardium predefinida denominada "QRadarPolicy" con tres reglas: una regla de bloqueo, una regla de alerta y una regla de registro. Cada regla está vinculada a su grupo correspondiente de la lista anterior.

Cómo instalar la solución QRadar y Guardium

Para obtener instrucciones completas sobre la instalación de la solución QRadar y Guardium, vaya al artículo de IBM Developerworks:

https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/W746177d414b9_4c5f_9095_5b8657ff8e9d/page/QRGuardium

Configuración de Guardium

Para que la solución QRadar y Guardium pueda autenticarse en la API REST de Guardium, se debe haber registrado en Guardium un ID de cliente y se debe haber obtenido el secreto de cliente asociado.

El registro de un ID de cliente se realiza utilizando el programa de utilidad de línea de mandatos grdapi de Guardium. Esta operación se realiza sólo una vez. El resultado del registro del ID de cliente es una entrada JSON que contiene detalles para el nuevo cliente, incluido el secreto del cliente.

```
> grdapi register_oauth_client client_id=qrguardium
ID=0
{"client_id":"qrguardium","client_secret":"3ac89782-ce55-
4f24-b795-b6c76ecc4045",
"grant_types":"password","scope":"read,write","redirect_uri"
:"https://joeApp"}
ok
```

Resolución de problemas de registros

La solución QRadar y Guardium proporciona varios archivos de registro como ayuda para gestionar y resolver problemas de las operaciones. Estos archivos de registro incluyen:

Tabla 1. Archivos de registro

Nombre del parámetro	Descripción
guardiumEvents_audit.log	Es un registro de auditoría de todos los cambios realizados en Guardium según los sucesos de QRadar. Cada línea es un objeto JSON que incluye identificadores, indicación de fecha y hora y detalles del suceso manejado.
QRListener.log	Salida del registro del proceso de escucha que recibe los datos de suceso enviados desde QRadar.
HANDLER_<nombre del suceso>.log	Salida de registro del manejador AL dedicado para un suceso específico.
RESPONSE_<nombre de suceso>.log	Salida de registro de una respuesta AL personalizada si este AL implementa el registro según su nombre AssemblyLine. Por ejemplo, esto se puede hacer estableciendo el parámetro Vía de acceso de archivo de adicionador de registro para que se calcule utilizando este Javascript: return “logs/” + task.getShortName() + “.log”;

Tema principal: Integración de productos
Información relacionada:
Integraciones del integrador de directorios (vídeo)

Interfaz de OPTIM a Guardium

Una interfaz de OPTIM a Guardium, que utiliza Protobuf (Universal Feed Agent), envía registros de actividad de Optim a Guardium.

El objetivo de esta interfaz es utilizar las funciones de auditoría de Guardium para las actividades de OPTIM. Las prestaciones de auditoría incluyen: herramientas de creación de informes (consultas e informes definidos por el usuario); procesos de auditoría (automatización de flujo de trabajo que permite asignar una tarea a un rol/usuario/grupo, proceso de flujo-estado definido por el usuario, escalamiento, exportación...) y alertas de umbrales.

La información de actividad de auditoría de Optim incluye los detalles de acceso, el número de sesión, el tipo de actividad (verbo), la tabla (objeto), los detalles (campos), el tiempo de ejecución (tiempo de respuesta) y el número de errores (registros afectados).

Los datos se correlacionan con el modelo de objetos estándar de Guardium.

La habilitación de la auditoría de OPTIM requiere la habilitación mediante OPTIM y los pasos necesarios en Guardium son: (1) enlazar el usuario al rol de auditoría de Optim; (2) añadir los informes predefinidos al panel adecuado; (3) habilitar el sniffer; y, (4) establecer la acción de política en Registrar datos con valores.

Esta interfaz incluye un rol de auditoría de Optim, un diseño predeterminado (archivo psml) para el rol de auditoría de optim y siete informes predefinidos.

Estos informes son:

- Optim - Resumen de solicitud fallida por servidor de Optim
- Optim - Ejecución de solicitud por usuario
- Optim Server Optim - Detalles del uso de la tabla
- Optim - Registro de solicitud
- Optim - Resumen del uso de la tabla
- Optim - Resumen de solicitudes

Nota: Al crear el usuario y el rol de optim-audit, sólo se mostrará un separador Auditoría de OPTIM. De forma similar a los roles con diseños personalizados que pueden generar los clientes, este es un diseño de rol que está pensado para utilizarse solo (el usuario de optim-audit no tiene ningún interés en los separadores de los otros usuarios) pero puesto que se requiere el rol de usuario, la fusión de diseño se ha desactivado cuando el usuario tiene el rol optim-audit, así que este verá sólo los elementos de optim que le interesan. Otros roles que funcionan de la misma forma son "review-only" e "inv".
Nota: Después de crear y guardar el rol optim-audit, pulse la selección Generar diseño en el menú del Explorador de usuarios y pulse Restablecer para obtener el diseño asociado al rol. Hágalo de nuevo si cambia los roles en el Explorador de usuarios.

Tema principal: Integración de productos

Combinación de alertas en tiempo real y análisis de correlación con productos SIEM

Distribuya el conocimiento contextual de los patrones, estructuras y protocolos de base de datos directamente a la base de datos de terceros del sistema SIEM.

Acerca de esta tarea

Guardium procesa previamente volúmenes grandes de tráfico de base de datos y destila la información importante. A continuación, proporciona el resumen condensado para los sistemas externos SIEM (Security Incident Event Manager) como, por ejemplo, ArcSight, Envision y QRadar. Por lo tanto, los productos SIEM no requieren trabajar tanto para procesar corrientes de tráfico grandes. En lugar de ello, pueden concentrarse en correlacionar toda la actividad, alertar sobre un comportamiento no autorizado o sospechoso y ayudar con los requisitos de cumplimiento normativo en los registros de sucesos.

Esta integración de Guardium SIEM (Security Incident Event Manager) se puede realizar de una de las maneras siguientes:

- Reenvío de Syslog (el método más común para sucesos y alertas)
- Utilizando el mandato de CLI, store remotelog, para especificar el reenvío de Syslog a recurso/prioridad, y host (destino).
- Utilizando plantillas de Guardium para ArcSight, Envision y QRadar
- SCP/FTP (archivos CSV o CEF enviados a un repositorio externo y que el sistema SIEM debe subir y analizar desde este repositorio externo).

Guardium distribuye su conocimiento contextual de patrones, estructuras y protocolos de base de datos directamente a la base de datos de terceros del sistema SIEM (Guardium tiene credenciales para el sistema SIEM). También puede escribir directamente en la base de datos SIEM en el esquema SIEM. Póngase en contacto con el soporte de Guardium ya que las entidades de Guardium deben estar correlacionadas con el esquema de terceros.

Nota: El sistema SIEM debe habilitar el registro remoto, así como saber estar a la escucha del recurso/prioridad correcto definido en syslog.

Combinando las alertas de seguridad en tiempo real y el análisis de correlación de Guardium con los productos de gestión de registros y SIEM, las empresas pueden mejorar su capacidad para:

- Identificar y mitigar los riesgos de forma proactiva frente a ataques externos, proveedores de confianza e infracciones de cumplimiento;
- Implementar controles automatizados de las normativas Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI-DSS) y de seguridad de datos;
- Gestionar sucesos del sistema y de la red junto con sucesos y registros críticos desde el núcleo de sus centros de datos: aplicaciones y bases de datos empresariales, para la correlación, el análisis forense, la priorización de incidencias y la creación de informes en toda la empresa.

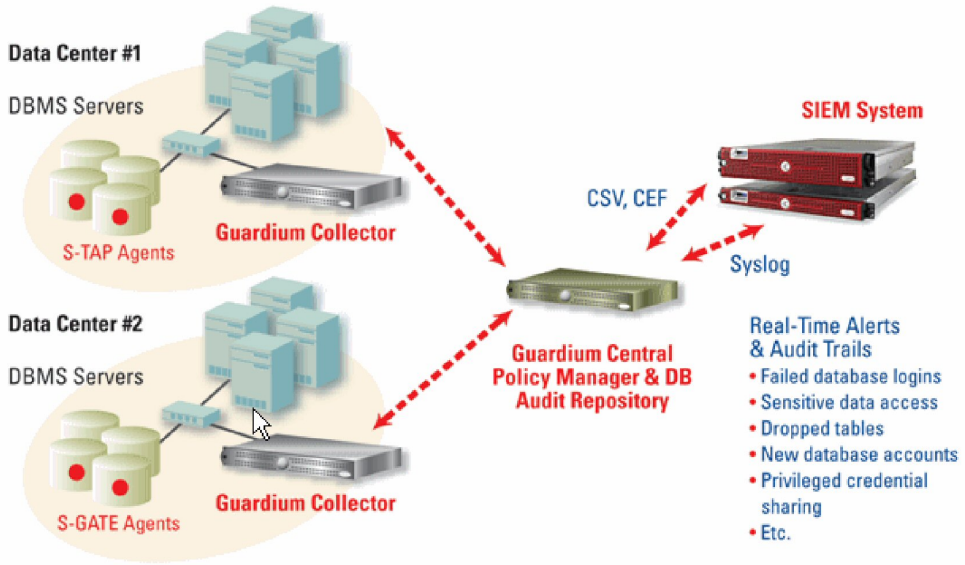
Las soluciones Security Information and Event Management (SIEM), también denominadas soluciones Security Event Management (SEM), las ofrecen empresas como por ejemplo QRadar, ArcSight, CA, Cisco MARS, LogLogic, RSA enVision y SenSage. Los productos SIEM son complementarios a la solución de supervisión de actividad de base de datos de Guardium. También pueden utilizar el filtrado y preproceso de Guardium de sucesos de base de datos para proporcionar visibilidad y análisis de base de datos completos para SOX, PCI-DSS y privacidad de datos.

La tecnología SIEM proporciona análisis en tiempo real de las alertas de seguridad generadas por las aplicaciones y el hardware de red. Ayuda a las empresas a responder más rápidamente a Los ataques de la red y a organizar las cantidades masivas de datos de registro que se generan a diario. Las soluciones SIEM son motores de correlación basados en registros.

Las soluciones SIEM se centran principalmente en la detección y la seguridad, pero no en la auditoría. Ensamblan datos de otros registros y los analizan a alto nivel. Correlacionan muchos más datos, como direcciones IP y direccionadores, pero tienen poca visibilidad de base de datos. No tienen funciones de supervisión de auditoría, firmadas digitalmente, con calidad de análisis forense, así que se pueden utilizar para obtener información inmediata, pero no para pruebas históricas.

Los usuarios de gestión de sucesos e información de seguridad (SIEM) se enfrentan al reto de importar registros en bruto generados por programas de utilidad de DBMS internos. El rendimiento de los programas de utilidad de registro DBMS, la información sin filtrar que generan y la falta de la información granular necesaria presentan retos.

Mediante la interfaz de usuario de Guardium, Guardium se puede configurar fácilmente para que se integre con diversas herramientas de SIEM.



Nota: Con la integración con SIEM, los informes y las políticas no cambian en el sistema Guardium. Los usuarios pueden continuar con sus políticas e informes existentes, desencadenar alertas y enviar informes al sistema SIEM.

Para la integración de SIEM y Guardium, hay plantillas predefinidas para QRadar, Envision y ArcSight, así que no es necesario que las defina. Puede seleccionar la plantilla de mensaje apropiada en la acción de regla.

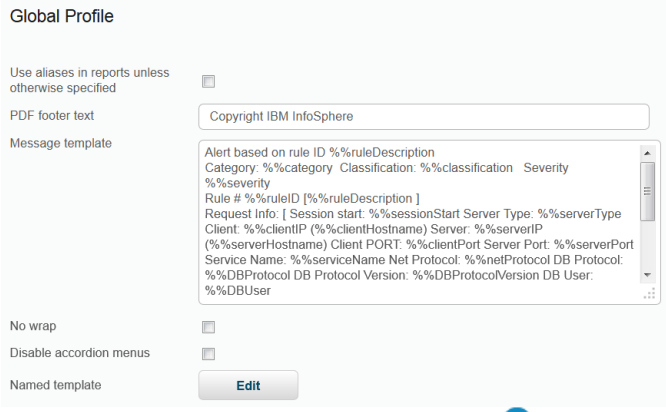
Puede modificar la plantilla de mensaje predeterminada, especificar los parámetros para el reenvío de syslog y crear el archivo CEF o CSV que se exportará.

Nota: Sólo se utiliza CEF para ArcSight. Los otros productos de SIEM tienen un formato diferente y no utilizan CEF.

Para que el producto SIEM reconozca la información que se está enviando, la plantilla de mensaje debe modificarse mediante el Perfil global. Este acuerdo de formato entre la solución de SIEM y Guardium permite a los productos de SIEM analizar los mensajes entrantes y actualizar su propia base de datos con los nuevos datos/sucesos.

1. Para abrir el Perfil global, pulse Configuración > Herramientas y vistas > Perfil global.

2. Pulse Editar para Plantilla con nombre.



3. Seleccione una plantilla o cree una plantilla nueva con el icono .

El dispositivo de Guardium se puede configurar para enviar mensajes de Syslog a sistemas remotos. Se pueden enviar tipos específicos de mensajes de Syslog a hosts específicos. El tipo de mensaje de Syslog se determina a partir de la prioridad de recurso del mensaje.

A continuación se muestran ejemplos de recursos: all, auth, authpriv, cron, daemon, ftp, kern, local0, local1, local2, local3, local4, local5, local6, local7, lpr, mail, mark, news, security, Syslog, user, uucp. A continuación se muestran ejemplos de prioridad: alert, all, crit, debug, emerg, err, info, notice, warning.

Los informes que contienen información que puede utilizar otras aplicaciones o informes que contienen grandes cantidades de datos se pueden exportar a un formato de archivo CSV. La salida de tarea de Informe, Seguimiento de auditoría de entidad y Conjunto de privacidad se puede exportar a archivos CSV (valores separados por comas). Además, la salida del archivo CSV se puede escribir en Syslog. Si se utiliza la capacidad de Syslog remoto, el archivo CSV de salida se reenvía a las ubicaciones de Syslog.

Cada registro de los archivos CSV o CEF representa una fila en el informe. Póngase en contacto con el soporte de Guardium para obtener una herramienta que permita el cambio de formato de los archivos CSV antes de la exportación.

El dispositivo de Guardium se puede configurar para enviar mensajes de Syslog a sistemas remotos, utilizando el mandato de CLI remotelog. Se pueden enviar tipos específicos de mensajes de Syslog a hosts específicos. El tipo de mensaje de Syslog se determina a partir de la prioridad de recurso del mensaje.

Ejemplos de recursos son: all, auth, authpriv, cron, daemon, ftp, kern, local0, local1, local2, local3, local4, local5, local6, local7, lpr, mail, mark, news, security, Syslog, user, uucp. Ejemplos de prioridad son: alert, all, crit, debug, emerg, err, info, notice, warning.

Los informes que contienen información que pueden utilizar otras aplicaciones, o informes que contienen grandes cantidades de datos, se pueden exportar a un formato de archivo CSV. La salida de tarea de Informe, Seguimiento de auditoría de entidad y Conjunto de privacidad se puede exportar a archivos CSV (valores separados por comas). Además, la salida del archivo CSV se puede escribir en Syslog. Si se utiliza la capacidad de Syslog remoto, esta acción da como resultado el reenvío inmediato del archivo CSV de salida a las ubicaciones remotas de Syslog.

Cada registro de los archivos CSV o CEF representa una fila en el informe.

Para enviar mensajes de Syslog y exportar informes a archivos CSV, realice los pasos siguientes.
Nota: No comprima los archivos en la definición de proceso de auditoría de forma que el proveedor de SIEM los pueda analizar correctamente.

1. Para abrir el Buscador de procesos de auditoría, pulse Cumplir > Herramientas y vistas > Creador de procesos de auditoría.
2. Pulse el icono para añadir un proceso o seleccione un proceso existente en la lista desplegable.
3. Pulse Nueva tarea de auditoría en Tareas de auditoría.
4. Especifique una descripción y seleccione Informe.
5. Seleccione un informe de la lista desplegable y especifique la etiqueta de archivo CSV/CEF.
6. Seleccione Exportar archivo CSV y Escribir en Syslog. Elija una plantilla con nombre en la lista desplegable.
7. En Parámetros de tarea, seleccione Especifique el periodo desde >= y Especifique el periodo hasta <= mediante el icono de calendario.
8. Pulse Aplicar.

Los archivos CSV/CEF también pueden exportarse en una planificación al host SIEM. Modifique o añada una tarea de auditoría.

1. Pulse Cumplir > Herramientas y vistas > Creador de procesos de auditoría para abrir el Buscador de procesos de auditoría y modificar o añadir una tarea de auditoría.
2. Elija Exportar archivo CSV o Exportar archivo CEF.
   Nota: Los informes ACCESO se pueden guardar y reenviar en formato CEF o LEEF, pero otros informes, como por ejemplo Inicios de sesión de Guardium, Registro de actividad de agregación o Sucesos CAS, no se pueden correlacionar con LEEF.
3. Deseleccione Escribir en Syslog. De lo contrario, se generarán mensajes de Syslog y no un archivo.
4. Abra el menú Exportar CSV/CEF pulsando Gestionar > Gestión de datos > Exportación de resultados (archivos).
5. Seleccione Protocolo SCP o FTP. A continuación, especifique Host, Directorio, Nombre de usuario, Puerto y Contraseña de SCP/FTP.
6. En la sección Planificación, defina la frecuencia de Hora de inicio, la frecuencia de Reiniciar, la frecuencia de Repetir, Planificar por Día/Semana o Mes, Hora de inicio planificada. Seleccione el recuadro para ejecutar automáticamente trabajos dependientes.
7. Pulse Guardar para confirmar los cambios o Restablecer para borrar los campos.

Para tener una alerta de política que se direccione a Syslog, las reglas de excepción, las reglas de acceso y las reglas de extrusión se deben modificar para que se desencadene el envío de notificaciones a Syslog. Para realizar esta acción, vaya al Creador de políticas. Las reglas de política se pueden enviar como correo electrónico o enviarse a Syslog y reenviarse.

1. Para abrir el Creador de políticas, pulse Configuración > Herramientas y vistas > Creador de políticas.
2. Seleccione la política y pulse Editar regla.
3. Pulse Añadir regla... > Añadir regla de excepción.
4. Especifique Descripción, Categoría, Clasificación y seleccione un nivel de Gravedad en la lista desplegable.

Para cada infracción de regla de política registrada durante el periodo de informe, el informe Infracciones de política proporciona la indicación de fecha y hora de la entidad Infracción de regla de política, Descripción de regla de acceso, IP de cliente, IP de servidor, Nombre de usuario de BD, Serie SQL completo de la entidad Infracción de regla de política, Descripción de gravedad y un recuento de infracciones para esa fila. Con este informe, los usuarios pueden agrupar las infracciones y crear incidencias, establecer la gravedad de cada infracción y asignar incidencias a los usuarios.

Tema principal: Integración de productos

Cómo transferir datos confidenciales a InfoSphere Discovery

Tome información de datos confidenciales, identificados y clasificados en IBM Security Guardium y transfiera esta información a InfoSphere Discovery.

Tanto IBM Guardium como InfoSphere Discovery tienen la capacidad de identificar y clasificar datos confidenciales como, por ejemplo, números de la seguridad social o números de tarjetas de crédito.

Un cliente del producto IBM Guardium puede utilizar una interfaz bidireccional para transferir información de datos confidenciales identificada de un producto a otro.

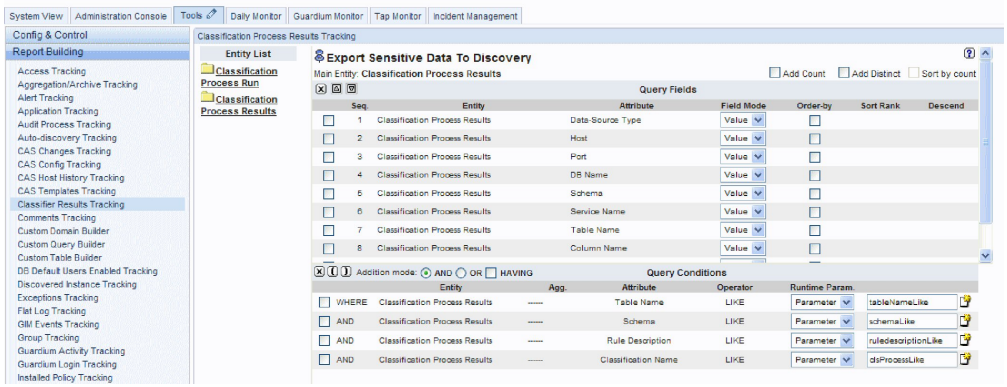
Nota: En IBM Guardium, el proceso Clasificación es un proceso continuado que se ejecuta periódicamente. En InfoSphere Discovery, Clasificación forma parte del proceso Descubrimiento que normalmente se ejecuta una vez.
Nota: Los datos se transferirán mediante archivos CSV.

El resumen de los procedimientos Exportar/Importar es el siguiente:

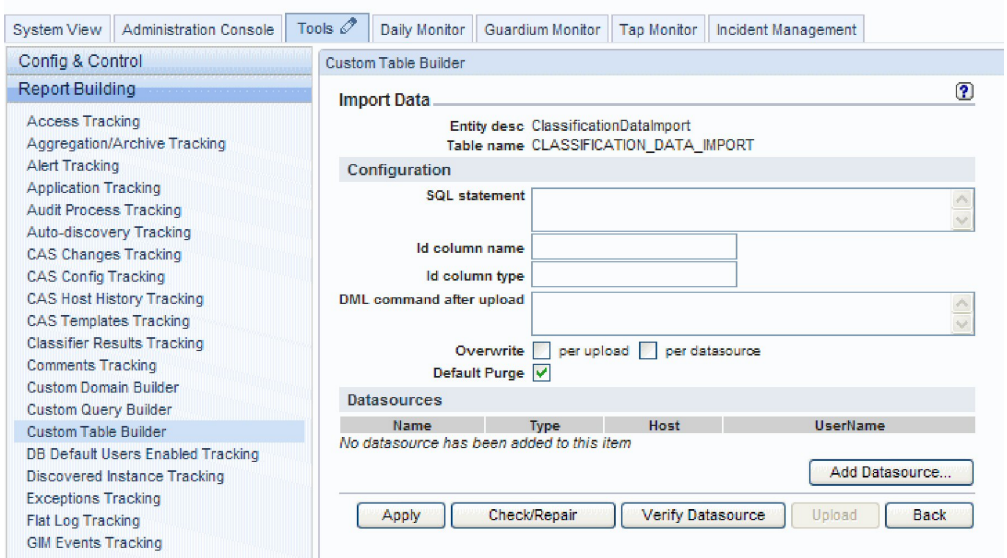
- Exportar desde Guardium: Ejecute el informe predefinido (Exportación de datos confidenciales a descubrimiento) y exporte como archivo CSV.
- Importar a Guardium: Cargue en una tabla personalizada para el origen de datos CSV; defina el informe predeterminado para este origen de datos.

Siga estos pasos:

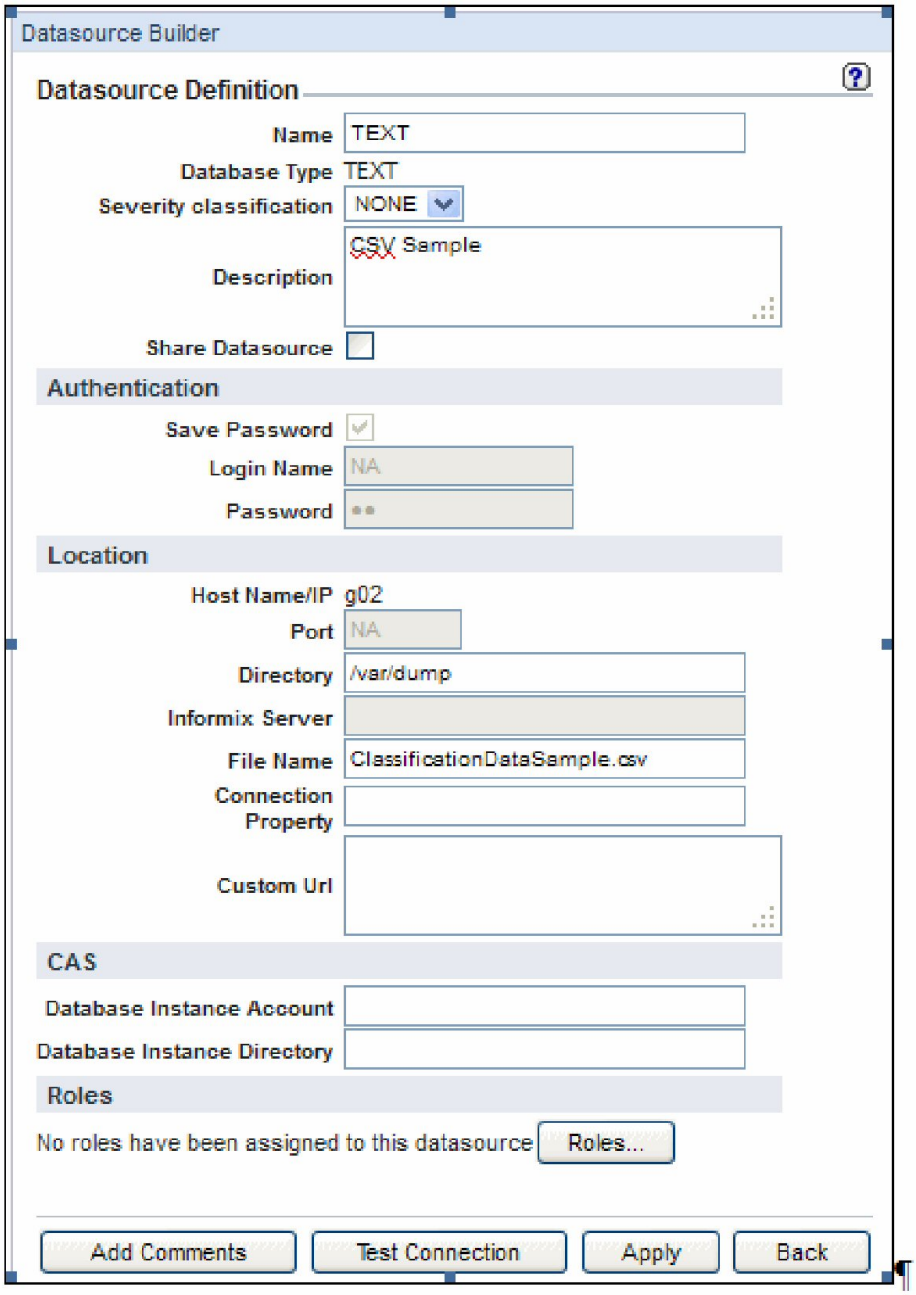
1. Exportar desde Guardium: Exporte datos de clasificación desde IBM Guardium a InfoSphere Discovery
2. Como usuario de administración en la aplicación Guardium, vaya a Herramientas > Creación de informes > Seguimiento de resultados de clasificador > Seleccione un informe > Exportación de datos confidenciales a descubrimiento (consulte la captura de pantalla).
   Nota: Añada este informe al panel de la interfaz de usuario (este no es el valor predeterminado).



3. Pulse un icono Personalizar en la pantalla Resultado del informe y especifique los criterios de búsqueda para filtrar los datos de resultados de la transferencia a descubrimiento.
4. Ejecute el informe y pulse el icono Descargar todos los registros.
5. Guarde como CSV e importe este archivo en descubrimiento de acuerdo con las instrucciones de InfoSphere Discovery.
6. Importar a Guardium: Importe datos de clasificación de InfoSphere Discovery a IBM Guardium
7. Exporte los datos de clasificación como CSV desde InfoSphere Discovery según las instrucciones de InfoSphere Discovery.
8. Como usuario de administración en la aplicación de Guardium, vaya a Herramientas > Creación de informes > pantalla Tablas personalizadas, seleccione ClassificationDataImport y pulse el botón Subir datos. (Consulte la captura de pantalla).



9. En la pantalla Subir datos, pulse Añadir origen de datos, pulse el botón Nuevo, defina el archivo CSV importado desde Discovery como nuevo origen de datos (Tipo de base de datos = Texto). Consulte la siguiente captura de pantalla de la definición de origen de datos CSV.



Nota: Como alternativa, puede cargar los datos directamente desde la base de datos de Discovery si sabe cómo acceder a ella y a los datos de resultados de clasificación.

10. Cuando haya definido el CSV como origen de datos, pulse el botón Añadir en la pantalla de la lista de orígenes de datos.
11. En la pantalla Subir datos, pulse Verificar origen de datos y, a continuación, Aplicar.
12. Pulse el botón Ejecutar una vez ahora para cargar los datos del archivo CSV.
13. Vaya al Creador de informes, seleccione el informe Importación de datos de clasificación, pulse Añadir al panel para añadirlo a su portal y, a continuación, vaya al informe.
14. Acceda al informe, pulse en Personalizar para establecer las fechas de inicio y finalización y ejecute el informe.

El resultado del informe tiene los datos de clasificación importados de InfoSphere Discovery. Efectúe una doble pulsación para invocar las API asignadas a este informe. Los datos importados de Discovery se pueden utilizar para:

- Añadir un nuevo origen de datos basado en el conjunto de resultados.
- Añadir/actualizar un grupo de datos confidenciales.
- Añada reglas de política basadas en la información de datos confidenciales y de origen de datos.
- Añadir un conjunto de privacidad.

Tabla 1. Firma de la interfaz de CSV

Firma de la interfaz	Ejemplo
Tipo	DB2
Host	9.148.99.99
Puerto	50001

Firma de la interfaz	Ejemplo
dbName (nombre de esquema para DB2 u Oracle, nombre de bd para otros)	cis_schema
URL de origen de datos	
TableName	MK_SCHED
ColumnName	ID_PIN
ClassificationName	SSN
RuleDescription	Algoritmo listo para usar de InfoSphere Discovery
HitRate	70 % - no disponible para la exportación en Guardium Vers. 8.2
ThresholdUsed	60 % - no disponible para la exportación en Guardium Vers. 8.2

Tema principal: Integración de productos

Correlación con CEF

El estándar CEF de ArcSight define un conjunto de campos necesarios y un conjunto de campos opcionales.

Estos últimos se denominan extensiones en el estándar CEF. Los datos se correlacionan con estos campos desde los informes e información de configuración de Guardium. Tenga en cuenta que no todos los campos de Guardium se correlacionan con un campo de CEF, por lo que puede que no haya una relación uno a uno entre las filas de un informe impreso y el archivo CEF generado para ese informe. Tenga en cuenta también que este recurso está pensado para correlacionar datos de dominios de acceso a datos (Acceso a datos, Excepciones e Infracciones de política, por ejemplo), y no de dominios de autosupervisión de Guardium (Agregación/Archivado, Proceso de auditoría, Inicios de sesión de Guardium, etc.).

Nota: La IP de cliente analizada tiene una correlación para el origen CEF. Si la consulta utilizada para CEF NO contiene la IP de cliente pero contiene la IP de cliente analizada, se utilizará la IP de cliente analizada para el origen. Si ambas se incluyen en la consulta, la IP de cliente tiene prioridad.

Los campos de CEF de la tabla siguiente siempre están presentes.

Tabla 1. Correlación de campos de CEF necesarios

Campo de CEF	Correlación de Guardium
Version	0 (cero); Actualmente la única versión para el formato CEF
Device Vendor	Guardium
Device Product	Guardium
Device Version	Número de versión del software de Guardium
Signature ID	ID de informe
Nombre	Título del informe
Severity	Código numérico en el rango 0-10, siendo 10 el suceso más importante. Si no se restablece en el informe, 0 (cero, que se convierte en Info para Guardium).

Los campos de extensión CEF son opcionales, y estarán presentes sólo cuando se aplique la correlación. Por ejemplo, si el informe no contiene una descripción de regla de acceso, el campo de acción (el primer campo de extensión) no estará presente. Para obtener información más detallada sobre las entidades y los atributos de Guardium, consulte el tema de referencia de la entidad correspondiente.

Tabla 2. Correlación con CEF, Guardium Versión 8.2

Campo de CEF	Entidad	Atributo
severity	Infracción de regla de política	Gravedad
act	Infracción de regla de política	Descripción de regla de acceso
app	Cliente/Servidor	Protocolo de BD
app	Excepción	Protocolo de base de datos
dst	Cliente/Servidor	IP de servidor
dst	Excepción	Dirección de destino
dhost	Cliente/Servidor	Nombre de host de servidor
dpt	Sesión	Puerto de servidor
dpt	Excepción	Puerto de destino
dproc	Cliente/Servidor	Programa fuente
duid	Cliente/Servidor	Usuario de SO
duser	Cliente/Servidor	Nombre de usuario de BD
duser	Excepción	Nombre de usuario
end	Excepción	Indicación de fecha y hora de excepción
end	Infracción de regla de política	Indicación de fecha y hora
end	Periodo de acceso	Final de periodo

Campo de CEF	Entidad	Atributo
end	Sesión	Fin de sesión
msg	Excepción	Descripción de la excepción
msg	Texto del mensaje	Texto del mensaje
msg	Texto del mensaje	Asunto del mensaje
src	Cliente/Servidor	IP de cliente
src	Cliente/Servidor	IP de cliente analizado
src	Excepción	Dirección de origen
shost	Cliente/Servidor	Nombre de host del cliente
smac	Cliente/Servidor	MAC cliente
spt	Sesión	Puerto de cliente
spt	Excepción	Puerto de origen
start	Excepción	Indicación de fecha y hora de excepción
start	Infracción de regla de política	Indicación de fecha y hora
start	Periodo de acceso	Inicio de periodo
start	Sesión	Inicio de sesión
proto	Cliente/Servidor	Protocolo de red
request	SQL COMPLETO	SQL Completo
request	SQL	SQL
cs1	Sesión	Cadena de UID
cs2	Sesión	Cadena de UID comprimida

Tabla 3. Correlación con CEF, Guardium Versión 9.0

Campo de CEF	Entidad	Atributo
severity	Infracción de regla de política	Gravedad
act	Infracción de regla de política	Descripción de regla de acceso
app	Cliente/Servidor	Protocolo de BD
app	Excepción	Protocolo de base de datos
dst	Cliente/Servidor	IP de servidor
dst	Excepción	Dirección de destino
dhost	Cliente/Servidor	Nombre de host de servidor
dpt	Sesión	Puerto de servidor
dpt	Excepción	Puerto de destino
dproc	Cliente/Servidor	Programa fuente
duid	Cliente/Servidor	Usuario de SO
duser	Cliente/Servidor	Nombre de usuario de BD
duser	Excepción	Nombre de usuario
end	Excepción	Indicación de fecha y hora de excepción
end	Infracción de regla de política	Indicación de fecha y hora
end	Periodo de acceso	Final de periodo
end	Sesión	Fin de sesión
msg	Excepción	Descripción de la excepción
msg	Texto del mensaje	Texto del mensaje
msg	Texto del mensaje	Asunto del mensaje
src	Cliente/Servidor	IP de cliente
src	Cliente/Servidor	IP de cliente analizado
src	Excepción	Dirección de origen
shost	Cliente/Servidor	Nombre de host del cliente
smac	Cliente/Servidor	MAC cliente
spt	Sesión	Puerto de cliente
spt	Excepción	Puerto de origen

Campo de CEF	Entidad	Atributo
start	Excepción	Indicación de fecha y hora de excepción
start	Infracción de regla de política	Indicación de fecha y hora
start	Periodo de acceso	Inicio de periodo
start	Sesión	Inicio de sesión
proto	Cliente/Servidor	Protocolo de red
request	SQL COMPLETO	SQL Completo
request	SQL	Sql
cs1	Sesión	Cadena de UID
cs2	Sesión	Cadena de UID comprimida

Para obtener más información sobre CEF, busque en la web Common Event Format: Event Interoperability Standard, o visite el sitio web de ArcSight: www.arcsight.com.

Tema principal: Integración de productos

Correlación LEEF

Log Event Extended Format (LEEF) de QRadar

El formato LEEF consta de una cabecera de syslog opcional, una cabecera LEEF y una serie de atributos que describen el suceso.

Syslog_Header(opcional) LEEF_Header|Event_Attributes

La cabecera LEEF se separa con una barra vertical ('|') y los atributos con tabuladores

Ejemplo

Jan 18 11:07:53 host LEEF:Version|Vendor|Product|Version|EventID|Key1=Value1<tabulador>Key2=Value2<tabulador>Key3=Value3<tabulador>... <tabulador>KeyN=ValueN

Tabla 1. Parámetros de LEEF

Parámetros	Descripción
LEEF: Version	Entero de versión que identifica la versión de LEEF que utiliza el mensaje de registro
Vendor	Serie que identifica el proveedor del dispositivo o aplicación que envía el registro de sucesos
Product	Serie de producto que identifica el producto que envía el registro de sucesos. Nota: La combinación de proveedor y producto debe ser exclusiva
Version	Serie que identifica la versión del dispositivo o de la aplicación que envía el registro de sucesos
EventID	ID que identifica el suceso de forma exclusiva
Attributes 1..N	Un conjunto de atributos de pares de clave-valor del suceso separados por el carácter de tabulación. El orden no se impone. Hay definido un conjunto predefinido de claves y se debe utilizar cuando sea posible. El formato LEEF es ampliable y permite añadir pares de clave-valor adicionales al registro de sucesos. Las claves no deben contener espacios o signos de igual Los valores no deben contener tabulaciones

Ejemplo:

```
Jan 18 11:07:53 192.168.1.1 LEEF:1.0|QRadar|QRM|1.0|NEW_PORT_DISCOVERD|src=172.5.6.67 dst=172.50.123.1 sev=5 cat=anomaly msg=there are spaces in this message
```

Codificación de caracteres

UTF8

Atributos predefinidos

Tabla 2. Atributos predefinidos

Nombre de clave	Tipo de datos	Longitud máxima	Descripción
Cat	serie		Categoría de suceso
devTime	fecha		Hora a la que el dispositivo o aplicación ha emitido el suceso
devTimeFormat	serie		Definido por SimpleDateFormat de java. Esto sólo es necesario si se utiliza un formato de fecha personalizado. Consulte la sección Formato de fecha para obtener más información.
proto	entero		Protocolo de transporte
sev	entero (1-10)		Gravedad de este suceso
src	Dirección IPv4 o IPv6		Dirección de origen
dst	Dirección IPv4 o IPv6		Dirección de destino

Nombre de clave	Tipo de datos	Longitud máxima	Descripción
VSrc	Dirección IPv4 o IPv6		Dirección de origen virtual
srcPort	entero		Puerto de origen. Los números de puerto válidos están entre 0 y 65535.
dstPort	entero		Puerto de destino. Los números de puerto válidos están entre 0 y 65535.
srcPreNat	Dirección IPv4 o IPv6		Dirección de origen para el mensaje antes de que se haya producido la conversión de direcciones de red (NAT)
dstPreNat	Dirección IPv4 o IPv6		Dirección de destino para el mensaje antes de que se haya producido la conversión de direcciones de red (NAT)
srcPostNat	Dirección IPv4 o IPv6		Dirección de origen para el mensaje después de que se haya producido la conversión de direcciones de red (NAT)
dstPostNat	Dirección IPv4 o IPv6		Dirección de destino para el mensaje después de que se haya producido la conversión de direcciones de red (NAT)
usrName	serie	255	Nombre de usuario asociado al suceso
srcMAC	Dirección MAC		Seis números hexadecimales separados por dos puntos. Ejemplo: `1:2D:67:BF:1A:71`
dstMAC	Dirección MAC		Seis números hexadecimales separados por dos puntos. Ejemplo: `11:2D:67:BF:1A:71`
srcPreNATPort	entero		Puerto de origen. Los números de puerto válidos están entre 0 y 65535.
dstPreNATPort	entero		Puerto de destino. Los números de puerto válidos están entre 0 y 65535.
srcPostNATPort	entero		Puerto de origen. Los números de puerto válidos están entre 0 y 65535.
dstPostNATPort	entero		Puerto de destino. Los números de puerto válidos están entre 0 y 65535.
identSRC	Dirección IPv4 o IPv6		
identHostName	serie	255	Nombre de host asociado con el suceso. Normalmente, este parámetro sólo está asociado con sucesos de identidad
identNetBios	serie	255	Nombre de NetBIOS asociado con el suceso. Normalmente, este parámetro sólo está asociado con sucesos de identidad
identGrpName	serie	255	Nombre de grupo asociado al suceso. Normalmente, este parámetro sólo está asociado con sucesos de identidad.

Atributos personalizados

En algunos casos, es posible que se necesiten atributos personalizados para identificar más información sobre el suceso que se está generando. En estos casos, los proveedores pueden definir sus propios atributos personalizados e incluirlos en el registro de sucesos. Los campos de atributos personalizados sólo se deben utilizar cuando no hay ninguna correlación aceptable en un campo predefinido.

Las claves de atributos personalizados deben ser:

- Una sola palabra sin espacios
- Alfanuméricas
- Claras y concisas
- No se les puede dar el mismo nombre que tenga una clave de atributo predefinido

Los atributos personalizados se pueden utilizar para su visualización en el Visor de sucesos de QRadar creando propiedades personalizadas.

Los atributos personalizados los puede utilizar el motor de informes de QRadar creando propiedades del cliente.

Los atributos personalizados NO se pueden utilizar para la correlación de sucesos

Nota: Añada databaseName=%%DBname a la plantilla LEEF para capturar el nombre de base de datos de MS-SQL. Actualice la plantilla LEEF existente o cree una nueva plantilla mediante la clonación.

Formatos de fecha

Puede utilizar cualquiera de estos formatos predefinidos:

1. Milisegundos desde el 1 de enero de 1970 (entero)
2. MMM dd aaaa HH:mm:ss, por ejemplo, Jun 06 2012 16:07:36
3. MMM dd aaaa HH:mm:ss.SSS, por ejemplo, Jun 06 2012 16:07:36.300
4. MMM dd aaaa HH:mm:ss.SSS zzz, por ejemplo, Jun 06 2012 02:07:36.300 GMT

Si estos formatos no son adecuados, puede definir un formato de fecha personalizado en el campo dTime especificando el formato de fecha utilizando la clave dTimeFormat.

Para obtener información adicional sobre cómo especificar un formato de fecha, visite la página de SimpleDateFormat en: http://java.sun.com/javase/6/docs/api/java/text/SimpleDateFormat.html

Tema principal: Integración de productos

Resolución de problemas

Para aislar y resolver problemas de productos de IBM, puede utilizar la información de soporte y de resolución de problemas. Esta información contiene instrucciones para utilizar los recursos de determinación de problemas que se proporcionan con los productos de IBM, incluido IBM Guardium.

- Técnicas de resolución de problemas
  La *resolución de problemas* es un procedimiento sistemático para resolver un problema. El objetivo de la resolución de problemas consiste en determinar por qué algo no funciona de la forma esperada y cómo resolver el problema. Algunas técnicas comunes pueden ayudar en la tarea de resolución de problemas.
- Problemas y soluciones
  Busque aquí soluciones a los problemas que se encuentre.

Técnicas de resolución de problemas

La *resolución de problemas* es un procedimiento sistemático para resolver un problema. El objetivo de la resolución de problemas consiste en determinar por qué algo no funciona de la forma esperada y cómo resolver el problema. Algunas técnicas comunes pueden ayudar en la tarea de resolución de problemas.

El primer paso en el proceso de resolución de problemas consiste en describir completamente el problema. Las descripciones de problema ayudan al usuario y al representante del soporte técnico de IBM a saber dónde empezar para encontrar la causa del problema. Este paso incluye la formulación de preguntas básicas:

- ¿Dónde están los síntomas del problema?
- ¿Dónde se produce el problema?
- ¿Cuándo se produce el problema?
- ¿En qué condiciones se produce el problema?
- ¿Se puede reproducir el problema?

Las respuestas a estas preguntas normalmente llevan a una buena descripción del problema, lo que a su vez puede llevarle a la resolución del problema.

¿Dónde están los síntomas del problema?

¿Cuál es el problema? Esta pregunta puede parecer sencilla, pero puede desglosarla en varias preguntas más específicas que creen una imagen más descriptiva del problema. Estas preguntas pueden incluir:

- ¿Quién o qué está informando del problema?
- ¿Cuáles son los códigos y los mensajes de error?
- ¿Cómo falla el sistema? Por ejemplo, ¿se trata de un bucle, el sistema se cuelga, disminuye el rendimiento o se obtiene el resultado incorrecto?

¿Dónde se produce el problema?

La determinación del origen del problema no siempre es fácil pero es uno de los pasos más importantes de la resolución de un problema. Pueden existir muchas capas de tecnología entre el componente que falla y el que informa del problema. Redes, discos y controladores son sólo algunos de los componentes a tener en cuenta cuando está investigando problemas.

Las preguntas siguientes le ayudan a centrarse en el lugar en el que se ha producido el problema para aislar la capa del problema:

- ¿El problema es específico de una plataforma o sistema operativo o es común entre varias plataformas o sistemas operativos?
- ¿Se da soporte a la configuración y al entorno actuales?
- ¿Todos los usuarios tienen el problema?
- (Para instalaciones multisitio.) ¿Todos los sitios tienen el problema?

Si una capa informa del problema, éste no tiene por qué originarse necesariamente en esa capa. Parte de la identificación de dónde se origina un problema consiste en entender el entorno en el que existe. Dedique algún tiempo a describir completamente el entorno del problema, incluida la información sobre el sistema operativo y la versión, todo el software y las versiones y el hardware. Confirme que está ejecutando en un entorno cuya configuración está soportada; muchos problemas pueden deberse a niveles de software incompatibles que no se pueden ejecutar conjuntamente o que no se han probado juntos en profundidad.

¿Cuándo se produce el problema?

Desarrolle una línea temporal detalla de los sucesos que han llevado a un error, especialmente en los casos en los que el error se ha producido una sola vez. La manera más fácil de desarrollar una línea temporal es retroceder: empiece en el momento en que se informó del error (de la forma más precisa posible, detallando incluso hasta el milisegundo) y vaya hacia atrás a través de los registros y la información disponibles. Normalmente debe retroceder sólo hasta el primer suceso sospechoso que se encuentre en un registro de diagnóstico.

Para desarrollar una línea temporal detallada de los sucesos, responda estas preguntas:

- ¿El problema se produce sólo en un momento determinado del día o de la noche?
- ¿Con qué frecuencia se produce el problema?
- ¿Qué secuencia de sucesos lleva al momento en que se informa del problema?
- ¿El problema se produce después de un cambio de entorno, como por ejemplo tras actualizar o instalar software o hardware?

La respuesta a estos tipos de preguntas puede darle un marco de referencia en el que investigar el problema.

¿En qué condiciones se produce el problema?

Una parte importante de la resolución de problemas es saber qué sistemas y aplicaciones se están ejecutando en el momento en que se produce un problema. Estas preguntas sobre su entorno le pueden ayudar a identificar la causa raíz del problema:

- ¿El problema siempre se produce cuando se está realizando la misma tarea?
- ¿Debe producirse una determinada secuencia de sucesos para que ocurra el problema?
- ¿Fallan otras aplicaciones simultáneamente?

La respuesta a estos tipos de preguntas puede ayudarle a explicar el entorno en el que se produce el problema y correlacionar las dependencias. Recuerde que el hecho de que se hayan producido varios problemas a la misma vez no significa que los problemas estén necesariamente relacionados.

¿Se puede reproducir el problema?

Desde el punto de vista de la resolución de problemas, el problema ideal es el que se puede reproducir. Normalmente, cuando un problema se puede reproducir, dispone de un conjunto de herramientas o procedimientos más amplio para ayudarle en la investigación. En consecuencia, los problemas que puede reproducir son a menudo más

fáciles de depurar y resolver.

No obstante, los problemas que pueden reproducirse pueden presentar una desventaja. Si el problema tiene un impacto considerable en el negocio, no desea que se vuelva a producir. Si es posible, vuelva a crear el problema en un entorno de prueba o desarrollo, que suele ofrecer más flexibilidad y control durante la investigación.

- ¿Se puede recrear el problema en un sistema de prueba?
- ¿Hay varios usuarios o aplicaciones que experimenten el mismo tipo de problema?
- ¿Se puede recrear el problema ejecutando un único mandato, un conjunto de mandatos o una aplicación determinada?

- Obtención de arreglos de Fix Central
  Puede utilizar Fix Central para buscar los arreglos recomendados por el soporte de IBM para diversos productos, incluido Guardium. Con Fix Central, puede buscar, seleccionar, pedir y descargar arreglos para su sistema y elegir las opciones de entrega. Es posible que exista un arreglo de producto para resolver su problema.
- Cómo ponerse en contacto con el soporte de IBM
  El soporte de IBM proporciona ayuda para los defectos del producto, responde a las preguntas más frecuentes y ayuda a los usuarios a resolver los problemas del producto.
- Información básica del soporte de IBM
  Antes de llamar al soporte de IBM, recopile información básica sobre IBM Guardium (recopilador, agregador, Gestor central; S-TAP UNIX/Linux; S-TAP Windows).
- Intercambio de información con IBM
  Para diagnosticar o identificar un problema, es posible que deba proporcionar datos e información de su sistema al soporte de IBM. En otros casos, es posible que el soporte de IBM le proporcione herramientas o programas de utilidad para la determinación de problemas.
- Suscripción a actualizaciones de soporte
  Para recibir información importante sobre los productos de IBM que utilice, puede suscribirse a las actualizaciones.

Tema principal: Resolución de problemas

Obtención de arreglos de Fix Central

Puede utilizar Fix Central para buscar los arreglos recomendados por el soporte de IBM para diversos productos, incluido Guardium. Con Fix Central, puede buscar, seleccionar, pedir y descargar arreglos para su sistema y elegir las opciones de entrega. Es posible que exista un arreglo de producto para resolver su problema.

Acerca de esta tarea

Procedimiento

Para buscar e instalar arreglos:

1. Obtenga las herramientas necesarias para obtener el arreglo. Si no está instalado, obtenga el instalador de actualización del producto. Puede descargar el instalador de Fix Central. Este sitio proporciona instrucciones de descarga, instalación y configuración para el instalador de actualizaciones.
2. Seleccione Guardium como el producto y marque uno o más recuadros de selección que sean relevantes para el problema que desea resolver.
3. Identifique y seleccione el arreglo que necesita.
4. Descargue el arreglo.
   a. Abra el documento de descarga y siga el enlace en la sección Descargar paquete.
   b. Cuando descargue el archivo, asegúrese de que el nombre del archivo de mantenimiento no haya cambiado. Este cambio puede ser intencionado o puede ser un cambio accidental debido a determinados navegadores web o programas de utilidad de descarga.
5. Aplique el arreglo.
   a. Siga las instrucciones de la sección Instrucciones de instalación del documento de descarga.
   b. Para obtener más información, consulte el tema Instalación de arreglos con el Instalador de actualizaciones de la documentación del producto.
6. Opcional: Suscríbase para recibir notificaciones de correo electrónico semanales sobre arreglos y otras actualizaciones del soporte de IBM.

Tema principal: Técnicas de resolución de problemas

Cómo ponerse en contacto con el soporte de IBM

El soporte de IBM proporciona ayuda para los defectos del producto, responde a las preguntas más frecuentes y ayuda a los usuarios a resolver los problemas del producto.

Antes de empezar

Después de intentar encontrar su respuesta o solución utilizando otras opciones de autoayuda como, por ejemplo, las notas técnicas, puede ponerse en contacto con el soporte de IBM. Antes de ponerse en contacto con el soporte de IBM, su empresa u organización debe tener un *nombre de contrato de mantenimiento* de IBM activo y debe estar autorizada para enviar problemas a IBM. Para obtener información sobre los tipos de soporte disponibles, consulte el tema Support portfolio del documento "*Software Support Handbook*".

Procedimiento

Para ponerse en contacto con el soporte de IBM sobre un problema:

1. Defina el problema, recopile la información general y determine la gravedad del problema. Para obtener más información, consulte el tema Getting IBM support de la publicación *Software Support Handbook*.
2. Recopile información de diagnóstico.
3. Envíe el problema al soporte de IBM de una de las maneras siguientes:
   - En línea a través del Portal de soporte de IBM: Puede abrir, actualizar y ver todas las solicitudes de servicio desde el portlet Solicitud de servicio en la página Solicitud de servicio.
   - Por teléfono: Para obtener el número de teléfono al que debe llamar en su zona, consulte la página web Directory of worldwide contacts.

Resultados

Si el problema enviado hace referencia a un defecto de software, a falta de documentación o a documentación inexacta, el soporte de IBM crea un APAR (Informe autorizado de análisis de programa). El APAR describe el problema en detalle. Siempre que sea posible, el soporte de IBM proporcionará una solución que podrá

implementar hasta que el APAR se resuelva y se proporcione un arreglo. IBM publica diariamente los APAR resueltos en el sitio web de soporte de IBM, de modo que otros usuarios que experimenten el mismo problema pueden beneficiarse de la misma resolución.
Tema principal: Técnicas de resolución de problemas
Información relacionada:
Cómo subir datos a un tíquet de soporte (PMR) (vídeo)
Resolución de problemas y soporte de Guardium (vídeo)

Información básica del soporte de IBM

Antes de llamar al soporte de IBM, recopile información básica sobre IBM Guardium (recopilador, agregador, Gestor central; S-TAP UNIX/Linux; S-TAP Windows).

Utilice mandatos support must_gather, que se puede ejecutar mediante la CLI para generar información específica sobre el estado de cualquier sistema Guardium. Esta información también se puede recopilar mediante la GUI de Guardium.

Esta información se puede subir desde el sistema Guardium y se puede enviar al soporte de IBM siempre que se registre un informe de gestión de problemas (PMR).

Recopilación de resultados de la información de soporte

Para recopilar la información de soporte, pulse Gestionar > Mantenimiento > Resultados de información de soporte. Complete las secciones siguientes.

1. Describa la sesión de recopilación de información de soporte.
2. Complete el número de PMR.
3. Para enviar los resultados a una dirección de correo electrónico, especifique Correo electrónico: y complete la dirección de correo electrónico.
4. Planifique una hora de inicio pulsando el icono de calendario.
5. Compruebe previamente que ha recopilado la información de registro relacionada con las categorías siguientes:
   - Agregación
   - Interfaz de usuario
   - Copia de seguridad
   - Usuario de BD
   - Planificador
   - Base de datos del sistema
   - Red
   - Salud del despliegue
   - Alerta
   - Auditoría
   - Gestor central
   - Depurar
   - Sniffer
   - Parche de instalación
   - Escaneado de amenazas avanzado
   - Optimización de titularidades
6. Especifique un valor para recopilar información para una determinada cantidad de tiempo en minutos. El valor predeterminado es 10 minutos. Este valor es el periodo de tiempo para el que se recopilarán los registros. Si especifica un correo electrónico, los registros se recopilan durante 10 minutos desde el momento en que se inicia el proceso y a continuación se envía un correo electrónico. Debe reproducir el problema y generar la información de registro durante el periodo de tiempo especificado para que los registros puedan contener la información de depuración necesaria para resolver los problemas.
7. Especifique el número máximo de filas que aparece en el archivo de registro de resultados.
8. Cuando haya terminado con la configuración, pulse Iniciar.
9. Vaya a Resultados de información de soporte para ver los resultados. Puede abrir o guardar el archivo .tgz.

Must Gather para el dispositivo de Guardium con la CLI

Recopilador, agregador o gestor central de IBM Guardium

El usuario puede ejecutar los mandatos must_gather en cualquier momento mediante la CLI. Realice los pasos siguientes.

1. Abra una sesión putty (o similar) al recopilador, agregador o gestor central correspondiente.
2. Inicie sesión como usuario `cli`.
3. En función del tipo de problema, pegue los mandatos must_gather relevantes en la solicitud de la CLI. Es posible que se necesite más de un mandato must_gather para diagnosticar el problema. Los mandatos se listan y se describen en la lista siguiente.
   - support must_gather agg_issues (proceso de agregación)
   - support must_gather alert_issues (alertas)
   - support must_gather app_issues (aplicación)
   - support must_gather audit_issues (proceso de auditoría)
   - support must_gather backup_issues (proceso de copia de seguridad)
   - support must_gather cm_issues (Gestor central)
   - support must_gather datamining_issues (minería de datos)
   - support must_gather miss_dbuser_prog_issues (usuario de base de datos del sistema)
   - support must_gather en (optimización de titularidad)
   - support must_gather network_issues (arquitectura de red)
   - support must_gather ocr_issues
   - support must_gather patch_install_issues (instalación y actualizaciones de parches)
   - support must_gather purge_issues (proceso de depuración)
   - support must_gather scheduler_issues (función de planificador)
   - support must_gather sniffer_issues (función de sniffer)
   - support must_gather system_db_info (rendimiento de espacio operativo o base de datos de sistema Guardium)

   La salida se escribe en el directorio must_gather con un nombre de archivo como el ejemplo siguiente:

   must_gather/system_logs/.tgz

4. Envíe la salida resultante al soporte de IBM.

   Mediante fileserver <dirección ip>, puede subir los archivos .tgz y enviarlos al soporte de IBM.

   Envíe el archivo mediante correo electrónico o súbalo a ECUREP utilizando la subida de datos estándar. Especifique el número y el archivo del PMR que se va a subir.

Must Gather para S-TAP UNIX/Linux

El script guard_diag genera estadísticas en el servidor que ayudan a Guardium con el diagnóstico.

Explicación de guard_diag:

Script de diagnóstico (guard_diag)

Visión general:

Ahora hay un script de diagnóstico (guard_diag) que se queda sin /usr/local/guardium/guard_stap/guard_diag cuando el registro de S-TAP se establece en el nivel 7 desde la interfaz gráfica de usuario. También es posible transferir este script a una máquina que ejecute S-TAP.

Uso: ./guard_diag output_dir

El script solicita la ubicación si el script no puede determinar automáticamente dónde está instalado S-TAP. El tiempo de ejecución es aproximadamente 1,5 minutos y si no se especifica ningún directorio de salida, el script coloca el archivo .tar generado en /tmp. Cuando el script se ejecuta y habilita el registro desde la interfaz gráfica de usuario, el archivo .tar se coloca en /var/tmp.

Datos generales del sistema recopilados:

- Uname -a
- Lista de módulos de kernel instalados
- Salida de un ciclo
- Tiempo de actividad
- Número y tipo de procesadores
- Volcado del syslog más reciente
- Salida de Netstat
- Lista de IPC
- Estadísticas de discos libres
- Copia de /etc/services
- Listado de directorios de /etc
- Diversa información específica de la plataforma
- Contenido de /etc/inittab

Datos de S-TAP recopilados:

- Versión de S-TAP
- Contenido de guard_tap.ini
- Ls -l en los nodos de dispositivo de K-TAP
- Rastreo de 30s de S-TAP
- Estadísticas de K-TAP
- Lista de todos los archivos del directorio de instalación
- K-TAP khash
- Registro de depuración detallada de K-TAP (2) y S-TAP (4)

Problemas conocidos:

- Tusc no está instalado en todos los sistemas operativos HP-UX, por lo que el rastreo del ID de S-TAP no funciona.
- gzip no está siempre instalado en el sistema. La retrotracción consiste en comprimir (extensión final de .tar.Z) y, si esto falla, colocar el archivo .tar en el directorio de salida.
- La salida de Topas en AIX se interpreta mejor mediante el terminal, puesto que contiene códigos de control que la hacen prácticamente ininteligible cuando se abre en un editor.
- El S-TAP no raíz presenta una serie de problemas relativos al script de diagnóstico.
- En Linux, /var/log/messages sólo es legible para root.
- Es posible que algunos sistemas operativos no se hayan configurado correctamente y esto haga que netstat muestre un error.
- La vía de acceso para el usuario no root es bastante básica y, como resultado, es posible que algunos mandatos no se ejecuten en absoluto. Notablemente, este problema conocido se produce en HP-UX con gzip.

Plataformas soportadas:

- Linux
- HP-UX
- AIX
- Solaris

Requisitos para STAP: Ninguno

Requisitos para Linux: Ninguno

Requisitos para AIX: Ninguno

Requisitos para Solaris: top, prtdiag, psrinfo

Requisitos para HP-UX: tusc

Must Gather para S-TAP Windows

La ejecución de este script genera los siguientes archivos de texto en el directorio actual:

- stap.txt
- tasks.txt
- system.txt
- evtlog.txt or evtlog2008.txt
- reg.txt

Notas:

1. Este script diag se puede ejecutar con cualquier versión de S-TAP.
2. Renombre el script diag a diag.bat y colóquelo en el directorio donde se ha instalado S-TAP. A continuación, puede ejecutarlo manualmente. Genera archivos de texto con información de diagnóstico.
3. Envíe los resultados al soporte de Guardium L3 o al equipo de investigación y desarrollo.

El script recopila los datos siguientes:

- El contenido de %system%guard_tap.ini.
- El registro de instalación de S-TAP de Guardium
- Todas las tareas en ejecución
- Lista de todos los controladores de kernel instalados
- Información del SO recopilada desde el programa de utilidad de información del sistema
- ipconfig /all
- netstat -nao
- Los resultados de ping y de rastreo del servidor de base de datos al sistema Guardium
- El uso de CPU de guardium_stapr
- El uso de CPU global del sistema
- El uso de memoria y el recuento de controladores de proceso de Guardium_stapr
- Los mensajes de registro de sucesos que genera S-TAP
- Los mensajes de registro de sucesos del sistema
- Las siguientes entradas de registro:
  - HKLMSOFTWAREMicrosoftWindowsCurrentVersionUninstall?
  - HKLMSYSTEMCurrentControlSetServices?
  - HKLMSYSTEMCurrentControlSetControlGroupOrderList?
  - HKEY_LOCAL_MACHINESOFTWAREMicrosoftMSSQLServer

Cifrar Must Gather

Cifrar Must Gather se ha añadido a la pantalla Perfil global. Para ir a la pantalla Perfil global, pulse Configuración > Perfil global. El valor predeterminado está deseleccionado (No cifrar). Si está deseleccionado, la salida Must Gather está comprimida y no se cifrada (función actual). Cuando el recuadro de selección está marcado, todas las futuras salidas Must Gather estarán cifradas. El cifrado se puede establecer mediante el mandato de CLI store encrypt_must_gather on y deseleccionar mediante el mandato store encrypt_must_gather off.

GuardAPI Must Gather

Utilice el mandato de GuardAPI para ejecutar la recopilación de GuardAPI Must Gather de información desde un script.

grdapi must_gather --help=true.

Se listan los siguientes parámetros de función.

```
ID=0
parámetros de función:
commandsList - Serie - necesario - Lista de valores de constante
description - Serie
email - Serie
maxLogLength - Entero - Lista de valores de constante
pmrNumber - Serie
runDuration - Entero - Lista de valores de constante
startRun - Fecha
Para obtener una lista de valores de constante para un parámetro, llame a la función con --get_param_values=<nombre-parám>
```

--commandsList requiere una serie. --description también es una serie necesaria. --runDuration indica que se ejecuta must_gather. Especifique una dirección de correo electrónico a la que se enviará el informe must_gather. El parámetro --maxLogLength es un entero necesario que establece la longitud máxima del informe de registro. --pmrNumber es el número de informe de gestión de problemas que utiliza el soporte de IBM para realizar un seguimiento de los informes de cliente y resolverlos. --startRun es una fecha necesaria, como ahora. Puede obtener una lista de valores para cada parámetro llamando a la función grdapi must_gather --get_param_values=<nombre-parám>.

Tema principal: Técnicas de resolución de problemas
Información relacionada:
Resolución de problemas y soporte de Guardium (vídeo)

Intercambio de información con IBM

Para diagnosticar o identificar un problema, es posible que deba proporcionar datos e información de su sistema al soporte de IBM. En otros casos, es posible que el soporte de IBM le proporcione herramientas o programas de utilidad para la determinación de problemas.
Tema principal: Técnicas de resolución de problemas

Envío de información al soporte de IBM

Para reducir el tiempo necesario para solucionar su problema, puede enviar información de rastreo y diagnóstico al soporte de IBM.

Procedimiento

Para enviar información de diagnóstico al soporte de IBM:

1. Abra un registro de gestión de problemas (PMR).
2. Recopile los datos de diagnóstico que necesita. Los datos de diagnóstico ayudan a reducir el tiempo que se tarda en resolver el PMR. Puede recopilar los datos de diagnóstico manual o automáticamente:
   - Recopile los datos manualmente.
   - Recopile los datos automáticamente.
3. Comprima los archivos utilizando el formato de archivo .zip o .tar.
4. Transfiera los archivos a IBM. Puede usar uno de los métodos siguientes para transferir los archivos a IBM:
   - La herramienta de solicitud de servicio
   - Métodos estándares de subida de datos: FTP, HTTP
   - Métodos seguros de subida de datos: FTPS, SFTP, HTTPS
   - Correo electrónico

   Todos estos métodos de intercambio de datos se explican en el sitio web de soporte de IBM.

Recepción de información del soporte de IBM

Ocasionalmente un representante del soporte técnico de IBM puede pedirle que descargue herramientas de diagnóstico u otros archivos. Puede utilizar FTP para descargar dichos archivos.

Antes de empezar

Asegúrese de que el representante del soporte técnico de IBM le haya proporcionado el servidor preferido que debe utilizarse para descargar los archivos y el directorio y los nombres de archivo exactos a los que debe acceder.

Procedimiento

Para descargar archivos del soporte de IBM:

1. Utilice FTP para conectarse al sitio que le ha indicado el representante de soporte técnico de IBM y conéctese como usuario `anonymous`. Utilice su dirección de correo electrónico como contraseña.
2. Vaya al directorio adecuado:
   a. Vaya al directorio /fromibm.

      ```
      cd fromibm
      ```

   b. Vaya al directorio que el representante del soporte técnico de IBM le ha proporcionado.

      ```
      cd nombrededirectorio
      ```

3. Habilite la modalidad binaria para la sesión.

   ```
   binary
   ```

4. Utilice el mandato get para descargar el archivo que ha especificado el representante de soporte técnico de IBM.

   ```
   get nombrearchivo.extensión
   ```

5. Finalice su sesión FTP.

   ```
   quit
   ```

Suscripción a actualizaciones de soporte

Para recibir información importante sobre los productos de IBM que utilice, puede suscribirse a las actualizaciones.

Acerca de esta tarea

Si se suscribe para recibir actualizaciones sobre Guardium, puede recibir información técnica importante y actualizaciones de recursos y herramientas de soporte de IBM. Puede suscribirse a las actualizaciones mediante uno de los procedimientos siguientes:

Suscripciones a redes sociales y canales de información RSS
: Estas disponibles las siguientes suscripciones a canales de información RSS y a redes sociales para Guardium:

  - *Canal de información RSS 1*
  - *Canal de información RSS 2*
  - *Canal de información RSS 3*

  Para obtener información general sobre RSS, incluyendo los pasos para comenzar y una lista de páginas web de IBM con RSS habilitado, visite el sitio de Canales de información RSS de soporte de software de IBM.

Mis notificaciones
: Con Mis notificaciones se puede suscribir a actualizaciones de soporte para cualquier producto de IBM. (Mis Notificaciones sustituye a Mi soporte, que es una herramienta similar que es posible que haya utilizado en el pasado.) Con Mis notificaciones, puede especificar que desea recibir diaria o semanalmente anuncios por correo electrónico. Puede especificar qué tipo de información desea recibir (como por ejemplo publicaciones, consejos y sugerencias, flashes de producto (también conocidos como alertas), descargas y controladores). Mis notificaciones permite personalizar y categorizar los productos sobre los que desea estar informado y los métodos de entrega que mejor se ajustan a sus necesidades.

Procedimiento

Para suscribirse a actualizaciones de soporte:

1. Suscríbase a los canales de información RSS de Guardium.

2. Para suscribirse a Mis notificaciones, vaya al Portal de soporte de IBM® y pulse Mis notificaciones en el portlet Notificaciones.
3. Regístrese utilizando su ID y contraseña de IBM, y pulse Enviar.
4. Identifique de qué y cómo desea recibir actualizaciones.
    a. Pulse el separador Suscribirse.
    b. Seleccione la marca de software o el tipo de hardware adecuados.
    c. Seleccione uno o más productos por su nombre y pulse Continuar.
    d. Seleccione sus preferencias sobre cómo recibir actualizaciones: por correo electrónico, en línea en una carpeta designada o como un canal de información RSS o Atom.
    e. Seleccione los tipos de actualizaciones de documentación que desea recibir, por ejemplo, nueva información sobre descargas de producto y comentarios de grupos de discusión.
    f. Pulse Enviar.

Resultados

Hasta que modifique sus preferencias de canales de información RSS y de Mis notificaciones, recibirá las notificaciones de las actualizaciones que haya solicitado. Puede modificar sus preferencias cuando sea necesario (por ejemplo, si deja de utilizar un producto y empieza a utilizar otro).

Tema principal: Técnicas de resolución de problemas

Información relacionada

Canales de alimentación RSS del soporte de software de IBM

Suscríbase a las actualizaciones de contenido de soporte de Mis notificaciones

Mis notificaciones para soporte técnico de IBM

Visión general de Mis notificaciones para soporte técnico de IBM

Problemas y soluciones

Busque aquí soluciones a los problemas que se encuentre.

- Interfaz de usuario
- Políticas
- Informes
- Evaluar y reforzar
- Configuración del sistema Guardium
- Gestión de acceso
- Agregación
- Gestión central
- S-TAP y otros agentes
- GIM
- Resolución de problemas de la actividad de archivos
- Instalación del sistema Guardium

Tema principal: Resolución de problemas

Interfaz de usuario

- Los cambios no se guardan cuando se añade un motor de inspección
  Si los cambios no se guardan cuando se añade un motor de inspección, compruebe que los parámetros sean válidos.
- Error HTTP 403
  Si recibe un error HTTP 403, puede inhabilitar la característica de protección contra la falsificación de solicitud entre sitios (CSRF, Cross-Site Request Forgery) para evitar el error.
- Java.lang.IllegalStateException
  Si se produce un error java.lang.IllegalStateException, limpie los servlets de Java.
- Las páginas no se están cargando correctamente
  Si las páginas no se cargan correctamente, reinicie la interfaz gráfica de usuario o utilice otro navegador.

Tema principal: Problemas y soluciones

Los cambios no se guardan cuando se añade un motor de inspección

Si los cambios no se guardan cuando se añade un motor de inspección, compruebe que los parámetros sean válidos.

Síntomas

Cuando se añade un motor de inspección, los nuevos valores permanecen durante unos minutos y, a continuación, desaparecen.

Causas

Hay un error en uno o más valores de parámetro con el nuevo motor de inspección o un motor de inspección distinto en el archivo de configuración de S-TAP guard_tap.ini.

Entorno

Afecta a la interfaz de usuario del recopilador de Guardium.

Resolución del problema

Compruebe que todos los parámetros que se deben establecer para el motor de inspección se hayan establecido en un valor válido. Por ejemplo, algunos tipos de base de datos requieren que establezca db_install_dir en la vía de acceso del directorio de instalación en el servidor. Sin embargo, para otros tipos de base de datos, este

parámetro no se debe establecer o debe establecerse en NULL. Compruebe los requisitos específicos para su tipo de base de datos en el Help Book de S-TAP y asegúrese de que todo esté correctamente establecido.

Tema principal: Interfaz de usuario

Error HTTP 403

Si recibe un error HTTP 403, puede inhabilitar la característica de protección contra la falsificación de solicitud entre sitios (CSRF, Cross-Site Request Forgery) para evitar el error.

Síntomas

Al renovar la interfaz gráfica de usuario de IBM Security Guardium desde la página principal del sistema, recibe el siguiente error:

```
HTTP Status 403-
type Status report
message
description Access to the specified resource () has been forbidden
```

Causas

La causa es una característica de Guardium diseñada para evitar la falsificación de solicitud entre sitios (CSRF). De forma predeterminada, la protección CSRF está habilitada.

Entorno

Afecta a todas las configuraciones de Guardium (recopilador, agregador, gestor central).

Resolución del problema

Puede inhabilitar esta característica utilizando el mandato de CLI siguiente: store gui csrf_status off

Nota: Si desactiva la protección de CSRF, el nivel de seguridad del sistema Guardium disminuye.

El mandato siguiente habilita la protección contra la falsificación de solicitud entre sitios. De forma predeterminada está habilitada: store gui csrf_status on

Puede comprobar el estado ejecutando este mandato de CLI: show gui csrf_status

Tema principal: Interfaz de usuario

Java.lang.IllegalStateException

Si se produce un error java.lang.IllegalStateException, limpie los servlets de Java.

Síntomas

Recibe el siguiente mensaje de error.

```
Se ha producido un error. Póngase en contacto con el administrador del sistema.
(java.lang.IllegalStateException)
```

Causas

El error se produce cuando se invoca un método y la máquina virtual Java está en un estado que no es coherente con el método. Es posible que también haya servlets Java dañados debido a puntos muertos.

Entorno

Afecta al sistema Guardium.

Resolución del problema

Espere unos minutos y vuélvalo a intentar. Si el error continúa, reinicie la interfaz gráfica de usuario iniciando sesión como usuario cli y ejecutando el mandato restart GUI.

Para limpiar los servlets de Java, ejecute el mandato support clean sevlets.

Si el problema no se ha resuelto, recopile los siguientes registros de tomcat y póngase en contacto con el soporte técnico de IBM Security Guardium.

```
tomcat_log/localhost.<inficación_fecha>.log
tomcat_log/catalina.<indicación_fecha>.log
```

Tema principal: Interfaz de usuario

Las páginas no se están cargando correctamente

Si las páginas no se cargan correctamente, reinicie la interfaz gráfica de usuario o utilice otro navegador.

Síntomas

Es posible que vea una pantalla en blanco u otros errores. Parece que el problema se produce con determinados navegadores en sistemas específicos, pero no con otros.

Causas

Es posible que la causa esté restringida a un navegador traducido o que haya un problema de máquina virtual Java.

Entorno

Afecta al recopilador, al agregador y al gestor central.

Resolución del problema

Para resolver el problema, ejecute restart GUI desde la solicitud de la CLI en el sistema Guardium. Si esto no ayuda, intente las acciones siguientes.

- Reinicie el sistema.
- Desinstale y vuelva a instalar la máquina virtual Java.
- Desinstale y vuelva a instalar el navegador.
- Utilice otro navegador.

Tema principal: Interfaz de usuario

Políticas

- La consulta no aparece en la definición de alerta de correlación
  Si la consulta no aparece en la definición de alerta de correlación, compruebe el campo de recuento y ordene por indicación de fecha y hora.
- La regla no se desencadena
  Si una regla con un valor en el campo de mandato de política no se desencadena de la forma esperada, reconfigure la regla.
- La función Redactar causa un resultado excesivamente enmascarado
  Si la función Redactar causa un resultado excesivamente enmascarado, utilice la expresión regular [\x0c]{1}[0-9]{8}([0-9]{4}).
- Las sesiones SSH y los trabajos CRON automatizados que inician sesión en la base de datos de Oracle se muestran como inicios de sesión fallidos.
  Si las sesiones SSH y los trabajos CRON automatizados que inician sesión en la base de datos de Oracle se muestran como inicios de sesión fallidos, modifique la política.
- La base de datos interna de Guardium se está llenando
  Si la base de datos interna de Guardium se está llenando, puede depurar los datos manualmente o como parte de la estrategia de depuración regular.

Tema principal: Problemas y soluciones

La consulta no aparece en la definición de alerta de correlación

Si la consulta no aparece en la definición de alerta de correlación, compruebe el campo de recuento y ordene por indicación de fecha y hora.

Síntomas

Ha creado una consulta de acceso para crear una alerta de correlación. Sin embargo, en la definición de alerta de correlación, esta consulta no aparece en la lista desplegable.

Causas

La búsqueda de alerta de correlación en el informe se basa en la indicación de fecha y hora.

Entorno

Afecta al recopilador y al agregador.

Resolución del problema

Marque el recuadro de selección Añadir recuento y ordene por indicación de fecha y hora.

Tema principal: Políticas

La regla no se desencadena

Si una regla con un valor en el campo de mandato de política no se desencadena de la forma esperada, reconfigure la regla.

Síntomas

Las reglas con un valor en el campo Mandato de política no se desencadenan como se espera.

Causas

La causa es una configuración incorrecta en el campo Mandato. El analizador de Guardium no considera que los modificadores de mandato formen parte de un mandato.

Entorno

Recopiladores de Guardium. También afecta al campo Mandato de la regla de política cuando se utiliza con el carácter comodín (%).

Resolución del problema

El valor del campo Mandato de la regla debe coincidir exactamente con un valor que se muestra en Verbo SQL, más un carácter comodín (%), según sea necesario. Este ejemplo es correcto.

```
GRANT
GRANT%
```

Este ejemplo es incorrecto.

```
GRANT% TO PUBLIC
%GRANT% ADMIN OPTION%
```

ADMIN OPTION y TO PUBLIC no coinciden y no pueden desencadenar una regla debido a que el analizador de Guardium no los reconoce como parte de un mandato. Normalmente, el analizador no considera que los modificadores de mandato formen parte de un mandato. En su lugar, cree un informe para inspeccionar el tráfico que supervisa la política e incluya el campo Verbo SQL de la entidad Mandato en dicho informe. El analizador reconoce todo lo que aparece en el campo Verbo SQL, que se puede utilizar en el campo Mandato de una regla de política. Se pueden añadir varios mandatos a un grupo, que se puede utilizar en la regla en lugar de un solo mandato. En este caso, cada miembro del grupo debe coincidir con una entrada en Verbo SQL. Guardium incluye varios grupos de mandatos de este tipo que se pueden utilizar o clonar.

Tema principal: Políticas
Tema principal: Informes

La función Redactar causa un resultado excesivamente enmascarado

Si la función Redactar causa un resultado excesivamente enmascarado, utilice la expresión regular [\x0c]{1}[0-9]{8}([0-9]{4}).

Síntomas

La función Redactar causa un resultado excesivamente enmascarado o un error ORA-03106 en el tráfico de Oracle.

Causas

La función Redactar de la regla de política de Guardium realiza una coincidencia de patrón con el conjunto de resultados. Tiene una característica para sustituir la serie coincidente con el carácter especificado por el usuario.

Entorno

Afecta a los recopiladores de Guardium.

Resolución del problema

Utilice la expresión regular `[\x0c]{1}[0-9]{8}([0-9]{4})`. Esta expresión regular garantiza que se inicia con la longitud de la columna seguida de 12 dígitos y sustituye los 4 últimos dígitos.

Tema principal: Políticas

Las sesiones SSH y los trabajos CRON automatizados que inician sesión en la base de datos de Oracle se muestran como inicios de sesión fallidos.

Si las sesiones SSH y los trabajos CRON automatizados que inician sesión en la base de datos de Oracle se muestran como inicios de sesión fallidos, modifique la política.

Síntomas

Las sesiones SSH y los trabajos automatizados CRON que inician sesión en la base de datos de Oracle mediante SQLPLUS y RMAN con `/as sysdba` se muestran como inicios de sesión fallidos.

Causas

Oracle responde a estos inicios de sesión con el siguiente error en tales intentos, incluso si no se muestra en la pantalla.

```
ORA-01-17: invalid username/password; logon denied.
```

Este error desencadena la alerta de inicio de sesión fallido. Por ejemplo, si el usuario de base de datos WRONGLOGIN es un miembro del grupo DBA e inicia sesión como `sqlplus WRONGLOGIN as sysdba`, la autenticación de la base de datos de WRONGLOGIN falla. Esta error hace que se desencadene la alerta de error ORA-01-17 y se refleje en el registro de Guardium. Sin embargo, los usuarios con privilegios sysdba se pueden conectar a la base de datos sin la autenticación de base de datos, por lo que la sesión puede continuar. Ambos sucesos se capturan y registran.

Entorno

Afecta a los recopiladores de Guardium.

Resolución del problema

Puede corregir la política para que incluya una acción de permitir antes de la regla que alerta sobre inicios de sesión fallidos. Cree una regla de excepción en la política con las condiciones siguientes.

```
Client IP=<IP del servidor>
Source program = SQLPLUS
DB user in trusted group
OS user in group of Oracle DBAs
Net protocol = BEQUEATH (if local BEQUEATH, not TCP)
```

Esta regla omite las alertas de inicio de sesión fallido causadas por el error ORA-01-17, pero aún se registran. Para filtrar las alertas de inicio de sesión fallidas de los informes, añada estas condiciones al final de la lista de condiciones:

```
AND
        (
    client IP<>IP del servidor OR
    prg orig <> SQLPLUS OR
    usuario bd NOT IN grupo de usuarios del so OR
    de confianza NOT IN grupo de DBA de oracle OR
    protocolo red <>BEQUEATH (si es local BEQUEATH, no TCP )
   )
```

Tema principal: Políticas

La base de datos interna de Guardium se está llenando

Si la base de datos interna de Guardium se está llenando, puede depurar los datos manualmente o como parte de la estrategia de depuración regular.

Síntomas

La base de datos interna de Guardium se está llenando y la mayoría de los datos están en la tabla GDM_POLICY_VIOLATIONS_LOG.

Causas

Un cambio en la política puede hacer que se desencadene con frecuencia una regla de infracción de política. Es posible que encuentre que la mayoría de los datos están almacenados en la tabla GDM_POLICY_VIOLATIONS_LOG.

Entorno

Afecta al recopilador de Guardium.

Diagnóstico del problema

Ejecute el mandato de CLI support show db-top-tables all.

Resolución del problema

Consulte el informe Infracciones de política/Gestión de incidentes para identificar qué regla de política se desencadena constantemente. A continuación, ajuste la regla de política para evitar que se desencadene tan a menudo.

El exceso de datos de la tabla GDM_POLICY_VIOLATIONS_LOG se depura como parte de la estrategia regular de depuración. Sin embargo, si desea limpiar manualmente datos de la tabla GDM_POLICY_VIOLATIONS_LOG, puede utilizar el mandato support clean DAM_data policy_violations<fecha_inicio><fecha_final>.

Tema principal: Políticas

Informes

- No puede modificar la tabla de receptor para un proceso de auditoría después de que se haya ejecutado al menos una vez
  Si no puede modificar la tabla de receptor para un proceso de auditoría, clone el proceso de auditoría y reemplace el original.
- No se pueden ver caracteres de varios bytes
  Si exporta un informe de Guardium a PDF y los caracteres no son correctos, cambie la configuración de font del PDF.
- El sistema de archivos está casi lleno
  Si el sistema de archivos Guardium está casi lleno, cambie la estrategia de rotación de archivos.
- Los informes de auditoría de Guardium visualizados en Microsoft Excel tienen filas con caracteres inesperados
  Si visualiza un informe de auditoría en .csv y ve filas con caracteres inesperados, utilice otro visor .csv o visualícelo como un archivo .pdf.
- Los informes muestran la dirección IP como 0.0.0.0
- Mensaje La solicitud se ha interrumpido o se ha excedido la cuota
  Si recibe un mensaje de error que indica que la solicitud se ha interrumpido o que se ha excedido la cuota al ejecutar un informe, divida el informe en fragmentos de un intervalo de informe más corto.
- La regla no se desencadena
  Si una regla con un valor en el campo de mandato de política no se desencadena de la forma esperada, reconfigure la regla.
- Excepciones de trabajos planificados cada 5 minutos
  Si recibe una excepción de trabajo planificado cada 5 minutos, desactive la alerta en la página Detección de anomalías.
- Excepción de trabajos planificados: Se requiere fusión, retardo al ejecutar proceso
  Si recibe un mensaje de error que indica Se requiere fusión, retardo al ejecutar proceso, vuelva a planificar el proceso de auditoría.
- El usuario de la base de datos no se muestra correctamente en los informes de Guardium cuando se supervisa Teradata
  Si los informes de Guardium no muestran correctamente el usuario de la base de datos al supervisar Teradata, configure la base de datos de Teradata.
- Resultados inesperados en informes de Guardium con mandatos incluidos
  Si recibe resultados inesperados en los informes de Guardium, configure las reglas de política para que manejen la profundidad mediante tuplas.

Tema principal: Problemas y soluciones

No puede modificar la tabla de receptor para un proceso de auditoría después de que se haya ejecutado al menos una vez

Si no puede modificar la tabla de receptor para un proceso de auditoría, clone el proceso de auditoría y reemplace el original.

Síntomas

Cuando un proceso de auditoría se ha ejecutado al menos una vez, no puede eliminar ni añadir un receptor. Tampoco puede modificar las propiedades siguientes de un receptor.

- Acción nec.
- Cont.
- Aprob. si vacío

Causas

Cuando un proceso de auditoría se ha ejecutado al menos una vez, la tabla de receptor se bloquea y no se puede modificar la mayoría de las propiedades.

Entorno

Afecta a todas las configuraciones de Guardium (recopilador, agregador, gestor central).

Resolución del problema

Los pasos siguientes le permiten modificar la tabla de receptor.

1. Clone el proceso de auditoría.
2. Realice cambios en el proceso de auditoría clonado.
3. Suprima el proceso de auditoría original. Sin embargo, si no desea perder el historial del proceso de auditoría, puede cambiar el nombre del proceso de auditoría.
4. Renombre el proceso de auditoría clonado con el nombre del proceso original.

Tema principal: Informes

No se pueden ver caracteres de varios bytes

Si exporta un informe de Guardium a PDF y los caracteres no son correctos, cambie la configuración de font del PDF.

Síntomas

Puede ver informes en la interfaz gráfica de usuario. Sin embargo, cuando exporta el informe a PDF, los caracteres no son correctos o faltan. Los caracteres aparecen como signos de interrogación u otros símbolos en el informe en PDF.

Causas

El font predeterminado de PDF en las exportaciones de PDF de Guardium PDF no muestra correctamente los caracteres de varios bytes. Por ejemplo, los caracteres griegos, cirílicos y chinos no se visualizan correctamente.

Entorno

Afecta al recopilador, al agregador y al gestor central.

Resolución del problema

En la versión 9 y posteriores, para resolver el problema cambie la configuración de fonts de PDF.

1. Inicie sesión como usuario en la CLI.
2. Ejecute el mandato store pdf-config multilanguage_support
3. Seleccione 2 Múltiples idiomas.

Tema principal: Informes

El sistema de archivos está casi lleno

Si el sistema de archivos Guardium está casi lleno, cambie la estrategia de rotación de archivos.

Síntomas

El sistema de archivos se está llenando y está próximo al 100 %.

Causas

Las alertas y los informes se envían al syslog y pueden llenar el sistema de archivos.

Entorno

Podría afectar al recopilador o agregador.

Resolución del problema

De forma predeterminada, los archivos de registro rotan semanalmente y mantienen cinco archivos. Sin embargo, puede cambiar la estrategia de rotación de registro de los archivos de registro. Utilice el mandato siguiente para mantener menos mensajes en el sistema.

```
store logrotate [agg|message] [daily|weekly|monthly] [# of rotations]
```

Tema principal: Informes

Los informes de auditoría de Guardium visualizados en Microsoft Excel tienen filas con caracteres inesperados

Si visualiza un informe de auditoría en .csv y ve filas con caracteres inesperados, utilice otro visor .csv o visualícelo como un archivo .pdf.

Síntomas

Cuando ve un informe de auditoría (en formato .csv) en Microsoft Excel, observa que determinadas filas se han llenado con caracteres inesperados. Los caracteres pueden ser similares a lo que se encuentra en la columna SQL completo. El problema no se ve en los informes .pdf ni en los informes de la interfaz gráfica de usuario.

Causas

Microsoft Excel limita lo que puede contener una celda a 32 767 caracteres. Si el SQL capturado tiene una longitud mayor que este límite, se extenderá a la fila siguiente.

Entorno

Afecta al recopilador, al agregador y al gestor central.

Resolución del problema

Utilice otro visor .csv que tenga un límite mayor de caracteres por celda o vea el informe de auditoría como un archivo .pdf.

Tema principal: Informes

Los informes muestran la dirección IP como 0.0.0.0

Síntomas

La dirección IP se muestra como 0.0.0.0. en Guardium.

Causas

Mientras que Guardium está descifrando el tráfico, la dirección IP se registra inicialmente como 0.0.0.0 porque el sniffer no sabe cuál es la dirección IP real. Una vez completada la descodificación, una hebra aparte vuelve a llenar las tablas de sesión con la dirección IP correcta.

Entorno

Afecta a cualquier base de datos que cifre el tráfico de base de datos.

Resolución del problema

Ejecute el mismo informe tras unos minutos. Para ver la IP de cliente correcta para el tráfico más reciente, añada el campo IP de cliente analizado desde el dominio de cliente/servidor al informe. Es posible que para algunas filas la IP de cliente analizado esté en blanco. Si está en blanco, el descifrado de esa sección de tráfico no se completa.

Tema principal: Informes

Mensaje La solicitud se ha interrumpido o se ha excedido la cuota

Si recibe un mensaje de error que indica que la solicitud se ha interrumpido o que se ha excedido la cuota al ejecutar un informe, divida el informe en fragmentos de un intervalo de informe más corto.

Síntomas

Cuando ejecuta un informe en Guardium, se recibe el siguiente mensaje de error. `La solicitud se ha interrumpido o se ha excedido la cuota`.

Causas

El mensaje de error `La solicitud se ha interrumpido o se ha excedido la cuota` aparece cuando un informe interactivo no se completa en el límite de tiempo de 3 minutos. La causa subyacente normalmente es el tamaño del informe.

Entorno

Afecta al recopilador y al agregador.

Resolución del problema

Para resolver el problema, complete una de las opciones siguientes.

- Divida el informe en fragmentos de un intervalo de informe más corto. Esta acción es el método más recomendado. Si un informe supera los 4 GB, se genera un agotamiento de tamaño de puntero de datos de tabla de MYSQL.
- Aumente el valor de tiempo de espera de consulta a un valor mayor. Pulse Gestionar > Supervisión de actividad > Supervisor de consultas en ejecución para abrir el Supervisor de consultas en ejecución.
- Desinstale y vuelva a instalar el navegador. Escriba un número de segundos en el recuadro Tiempo de espera de informe/supervisor de consultas y pulse Actualizar.

- Ejecute el informe en segundo plano. Los informes que se ejecutan en segundo plano no están sujetos al tiempo de espera de consulta.
- Ejecutar el informe como un proceso de auditoría.

Tema principal: Informes

La regla no se desencadena

Si una regla con un valor en el campo de mandato de política no se desencadena de la forma esperada, reconfigure la regla.

Síntomas

Las reglas con un valor en el campo Mandato de política no se desencadenan como se espera.

Causas

La causa es una configuración incorrecta en el campo Mandato. El analizador de Guardium no considera que los modificadores de mandato formen parte de un mandato.

Entorno

Recopiladores de Guardium. También afecta al campo Mandato de la regla de política cuando se utiliza con el carácter comodín (%).

Resolución del problema

El valor del campo Mandato de la regla debe coincidir exactamente con un valor que se muestra en Verbo SQL, más un carácter comodín (%), según sea necesario. Este ejemplo es correcto.

```
GRANT
GRANT%
```

Este ejemplo es incorrecto.

```
GRANT% TO PUBLIC
%GRANT% ADMIN OPTION%
```

ADMIN OPTION y TO PUBLIC no coinciden y no pueden desencadenar una regla debido a que el analizador de Guardium no los reconoce como parte de un mandato. Normalmente, el analizador no considera que los modificadores de mandato formen parte de un mandato. En su lugar, cree un informe para inspeccionar el tráfico que supervisa la política e incluya el campo Verbo SQL de la entidad Mandato en dicho informe. El analizador reconoce todo lo que aparece en el campo Verbo SQL, que se puede utilizar en el campo Mandato de una regla de política. Se pueden añadir varios mandatos a un grupo, que se puede utilizar en la regla en lugar de un solo mandato. En este caso, cada miembro del grupo debe coincidir con una entrada en Verbo SQL. Guardium incluye varios grupos de mandatos de este tipo que se pueden utilizar o clonar.
Tema principal: Políticas
Tema principal: Informes

Excepciones de trabajos planificados cada 5 minutos

Si recibe una excepción de trabajo planificado cada 5 minutos, desactive la alerta en la página Detección de anomalías.

Síntomas

Se recibe el mismo mensaje en el informe Excepciones de trabajos planificados a cortos intervalos regulares, normalmente cada 5 minutos. Este intervalo es el mismo que el intervalo de sondeo con el que se ejecuta la detección de anomalías.

Un ejemplo del informe Excepciones de trabajos planificados puede tener un aspecto similar al siguiente.

```
Indicación de fecha y hora            Descripción de la excepción                        Recuento de excepciones
2013-12-05 15:51:22.0 java.lang.NumberFormatException: empty String        1
```

La misma excepción aparece cada 5 minutos.

Causas

Una de las alertas activas está causando el error.

Entorno

Afecta a los recopiladores y al agregador de Guardium.

Diagnóstico del problema

Puede comprobar el intervalo de sondeo y las alertas activas en la página Detección de anomalías. Pulse Proteger > Detección de intrusiones en base de datos > Detección de anomalías para abrir la página Detección de anomalías.

Resolución del problema

Identifique la alerta exacta que está causando el problema y desactívela.

1. Desactive una alerta en la página Detección de anomalías.
2. Espere a que transcurra el intervalo de sondeo.
3. Compruebe si los errores se detienen con esa alerta desactivada.

4. Si no es así, reactive la alerta y desactive la siguiente.
5. Repita los pasos 2-5 hasta que haya probado con todas las alertas.

Si encuentra la alerta que está causando el problema y necesita ayuda para entender o detener el error, póngase en contacto con el soporte técnico de IBM Guardium y proporcione los siguientes elementos:

1. El texto exacto y la captura de pantalla del error.
2. La salida de los siguientes mandatos de CLI. Si se le solicita, especifique la duración de un intervalo de sondeo.

   support must_gather app_issues

   support must_gather alert_issues

Tema principal: Informes

Excepción de trabajos planificados: Se requiere fusión, retardo al ejecutar proceso

Si recibe un mensaje de error que indica Se requiere fusión, retardo al ejecutar proceso, vuelva a planificar el proceso de auditoría.

Síntomas

Recibirá el mensaje siguiente.`Se requiere fusión, retardo al ejecutar proceso`. Es posible que reciba varios de estos errores en un breve periodo de tiempo.

Causas

El proceso de auditoría requiere que el proceso de fusión finalice antes de que se puede ejecutar.

Entorno

Afecta al agregador.

Diagnóstico del problema

Pulse Informes > Informes operativos de Guardium > Registro de agregación/archivado para abrir el Registro de agregación/archivado.También puede diagnosticar el problema en agg_progress.log.

Resolución del problema

Vuelva a planificar el proceso de auditoría para que se ejecute al menos 10 minutos después del proceso de fusión.

Tema principal: Informes

El usuario de la base de datos no se muestra correctamente en los informes de Guardium cuando se supervisa Teradata

Si los informes de Guardium no muestran correctamente el usuario de la base de datos al supervisar Teradata, configure la base de datos de Teradata.

Síntomas

Cuando visualiza registros de la base de datos de Teradata supervisada en informes de Guardium, el campo de nombre de usuario de base de datos no se muestra como se esperaba. El nombre de usuario está truncado o falta.

Causas

La base de datos de Teradata no está habilitada para devolver el nombre de usuario completo.

Entorno

Afecta a cualquier recopilador de Guardium que capture datos de la base de datos de Teradata.

Resolución del problema

Utilice el mandato siguiente para permitir la base de datos de Teradata devuelva el nombre de usuario completo, en el juego de caracteres correcto, a la aplicación de supervisión. No afecta a otras aplicaciones.

gtwcontrol -u yes -d

El mandato -d muestra los valores de GDO actualizados.

Nota: Esta configuración devuelve el nombre de usuario en formato no cifrado. Si el cifrado está habilitado, el sistema devuelve un mensaje de error.
Tema principal: Informes

Resultados inesperados en informes de Guardium con mandatos incluidos

Si recibe resultados inesperados en los informes de Guardium, configure las reglas de política para que manejen la profundidad mediante tuplas.

Síntomas

Ve resultados inesperados en los informes o que cree que la política debería filtrar. En cambio, no se capturan las sentencias que espera que se capturen.

Causas

El SQL normalmente tiene varios objetos y mandatos incluidos en la sentencia. La definición de informe o de política no está configurada para tratar objetos o mandatos a distinta profundidad.

Entorno

Afecta a los recopiladores de Guardium.

Resolución del problema

Verifique que las condiciones coinciden con el nombre de objeto correcto. Utilice la entidad principal correcta para mostrar objetos o verbos SQL a distinta profundidad. Si aún ve un comportamiento inesperado, utilice el creador de grupos para definir un grupo de tuplas que se utilizará en la política. Una tupla permite que varios atributos se combinen para formar un único miembro de grupo.

Nota: La tupla da soporte al uso de una barra inclinada y de un carácter comodín (%). No da soporte al uso de una barra inclinada doble.
Tema principal: Informes

Evaluar y reforzar

- CAS no funciona con Java 1.7 en Windows
  Si el sistema de auditoría de cambios (CAS) de Guardium no funciona con Java versión 1.7 en Windows, copie msvcr100.dll en la carpeta bin de CAS.
- Miembros del grupo de excepciones Asesoramiento de vulnerabilidades aparecen en la prueba fallida
  Si aparecen miembros de un grupo de excepciones de prueba en una prueba de asesoramiento de vulnerabilidades fallida, utilice una secuencia de escape para el carácter de barra inclinada invertida.

Tema principal: Problemas y soluciones

CAS no funciona con Java 1.7 en Windows

Si el sistema de auditoría de cambios (CAS) de Guardium no funciona con Java versión 1.7 en Windows, copie msvcr100.dll en la carpeta bin de CAS.

Síntomas

CAS de Guardium funciona con versiones anteriores de Java pero no con Java 1.7.

Causas

Falta msvcr100.dll en <Directorio de STAP de GUARDIUM>\cas\bin\

Entorno

Afecta a CAS de Guardium en Windows.

Resolución del problema

Para resolver el problema, realice los pasos siguientes.

1. Busque la vía de acceso en la que está instalado Java 1.7 en el sistema, como por ejemplo C:\Program Files (x86)\Java\jre7\bin
2. Busque la ubicación de la biblioteca jvm.dll en la vía de acceso de Java que se ha encontrado en el paso anterior.
3. Edite el archivo cas.cfg en el directorio <directorio de CAS>\conf. Por ejemplo, C:\Program Files (x86)\GUARDIUM_STAP\cas\conf\cas.cfg es una vía de acceso de archivo típica.
4. Busque la línea correspondiente a la JVM como, por ejemplo, ;JVM=c:\program files\java\jre1_2_3\bin\client\jvm.dll.
5. Elimine el punto y coma del principio de la línea. A continuación, establezca la JVM en la vía de acceso de la biblioteca jvm.dll en el paso 2. `JVM=C:\Program Files (x86)\Java\jre7\bin\server\jvm.dll`.
6. Copie msvcr100.dll de la carpeta bin del directorio de instalación de Java 7 en la carpeta <directorio de CAS>\bin. Por ejemplo, copie C:\Program Files (x86)\Java\jre7\bin\msvcr100.dll en C:\Program Files (x86)\Guardium\GUARDIUM_STAP\cas\bin\msvcr100.dll.
7. Reinicie el sistema de auditoría de cambios.

Nota: Esto sólo es necesario para Java versión 1.7. Para versiones anteriores de Java, este paso no es necesario.
Tema principal: Evaluar y reforzar

Miembros del grupo de excepciones Asesoramiento de vulnerabilidades aparecen en la prueba fallida

Si aparecen miembros de un grupo de excepciones de prueba en una prueba de asesoramiento de vulnerabilidades fallida, utilice una secuencia de escape para el carácter de barra inclinada invertida.

Síntomas

Algunos miembros de un grupo de excepciones de prueba aparecen en el campo de detalles cuando se ejecuta un asesoramiento de vulnerabilidades. El grupo contiene miembros con un carácter de barra inclinada invertida y un código REGEX como por ejemplo `(R)US\John Doe`.

Causas

Los caracteres especiales pueden desencadenar errores cuando Guardium analiza el grupo de excepciones.

Entorno

Afecta a los recopiladores de Guardium.

Resolución del problema

Utilice una secuencia de escape para el carácter de barra inclinada invertida o no utilice el código REGEX (utilice una coincidencia exacta). Cualquiera de estos dos ejemplos funciona.

```
US\John Doe
```

```
(R)US\\John Doe
```

El código REGEX (R) se utiliza para desencadenar una búsqueda de expresión regular del campo de detalles para eliminar cualquier serie que coincida con la expresión regular. Una barra inclinada invertida o cualquier otro carácter que tenga un significado en una expresión regular necesita una secuencia de escape de barra inclinada invertida para evitar errores de análisis. Si no utiliza el código (R), el miembro del grupo debe coincidir exactamente con toda la línea en el campo de detalles de Guardium para encontrar una coincidencia. Para pasar la prueba de vulnerabilidades, el campo de detalles de la prueba debe estar vacío.

Tema principal: Evaluar y reforzar

Configuración del sistema Guardium

- No se puede configurar STAP después de la actualización
  Configure S-TAP en Guardium después de actualizar S-TAP.
- Guardium no puede reconocer el dispositivo de red VMXNET x
  Si Guardium no puede reconocer el dispositivo de red VMXNET x, instale Guardium en una máquina virtual y añada el adaptador de red.
- Error de interfaz de red de Guardium después de sustituir la placa del sistema
  Si recibe un mensaje de error después de una reparación de hardware, restablezca los parámetros de red.
- La máquina virtual Guardium no es accesible desde la red
  Si la máquina virtual Guardium no es accesible desde la red, ejecute el inventario de interfaz de red de almacén de mandatos y reinicie el sistema.
- SSLv3 está habilitado
  Si recibe un aviso de que `SSLv3 está habilitado`, inhabilite SSLv3 para evitar que se aproveche POODLE.

Tema principal: Problemas y soluciones

No se puede configurar STAP después de la actualización

Configure S-TAP en Guardium después de actualizar S-TAP.

Síntomas

Después de actualizar S-TAP utilizando Guardium Installation Manager (GIM), no puede configurar los parámetros de vía de acceso de base de datos en el motor de inspección de Guardium, aunque los resultados de la instalación del módulo se muestran como correctos.

Causas

K-TAP no se actualiza correctamente si el nuevo S-TAP está instalado como un módulo nuevo. Puesto que el módulo K-TAP anterior no se elimina, existe una discrepancia de protocolo entre el módulo K-TAP anterior y el nuevo S-TAP.

Entorno

S-TAP instalado en UNIX y Linux como, por ejemplo, AIX, HP-UX, Linux y Solaris.

Diagnóstico del problema

Para diagnosticar el problema, ejecute el programa de utilidad guard_diag para recopilar los datos para S-TAP de Guardium.

en el archivo syslog se ven las líneas siguientes.

```
STAP and KTAP Protocol Version Mismatch,
Exit!!!!!: No such file or directory
Tap_controller::init failed
GUARD-01: Error Initializing STap
```

El archivo de registro de módulos lista el K-TAP anterior. Por ejemplo: `ktap_24276 338760 0`

Resolución del problema

Para resolver el problema, siga estos pasos en el panel de instalación de módulos de GIM.

1. Establezca K-TAP Live Update en Y.
2. Establezca K-TAP_ENABLED en Y y vuelva a instalar el nuevo S-TAP.

Tema principal: Configuración del sistema Guardium

Guardium no puede reconocer el dispositivo de red VMXNET x

Si Guardium no puede reconocer el dispositivo de red VMXNET x, instale Guardium en una máquina virtual y añada el adaptador de red.

Síntomas

Guardium no puede reconocer el dispositivo de red VMXNET x durante la instalación en VMware. Recibe el error `eth0: unknown interface: No such device` cuando instala Guardium on VMware como invitado. El mensaje de error aparece después de reiniciar el sistema.

Causas

El adaptador de red virtual VMXNET x requiere un controlador específico que sólo está contenido en herramientas de VMware y ningún sistema operativo tiene el controlador. Guardium se está ejecutando en Linux y el instalador no tiene un controlador para VMXNET x.

Entorno

Afecta al sistema Guardium.

Resolución del problema

Resuelva el problema realizando los pasos siguientes.

1. Cree una máquina virtual en VMware utilizando un adaptador de red predeterminado, por ejemplo E1000 o Flexible.
2. Instale Guardium en la máquina virtual.
3. Instale el parche acumulativo actual de GPU para Guardium.
4. Después de la instalación, inicie sesión en la consola de CLI y ejecute el mandato setup vmware_tools install para instalar las herramientas de VMware.
5. Concluya el sistema Guardium desde la consola de CLI con el mandato stop system.
6. Edite los valores de la máquina virtual con una herramienta de cliente de VMware como, por ejemplo, el cliente de VMware Infraestructure. Seleccione el adaptador de red actual y elimínelo.
7. Añada el adaptador de red denominado VMXNET.
8. Reinicie el sistema Guardium.

Tema principal: Configuración del sistema Guardium

Error de interfaz de red de Guardium después de sustituir la placa del sistema

Si recibe un mensaje de error después de una reparación de hardware, restablezca los parámetros de red.

Síntomas

Después de una reparación de hardware como, por ejemplo, sustituir la placa del sistema en el dispositivo de Guardium, la conectividad de red se pierde. Cuando se rearranca el dispositivo, aparece el siguiente mensaje de error para cada interfaz de red.

```
rtnetlink answers: no such device
```

Causas

Después de sustituir la placa del sistema, la dirección MAC cambiará. Este cambio causa una disparidad entre la dirección MAC real y la que se almacenada en los archivos de configuración de la interfaz.

Entorno

Afecta a todos los dispositivos de Guardium (recopilador, agregador o gestor central) en los que se ha sustituido la placa del sistema y a todas las versiones de Guardium.

Resolución del problema

Inicie sesión en el dispositivo desde la consola como usuario CLI y restablezca los parámetros de red ejecutando los mandatos siguientes.

```
store network interface inventory
restart network
store network interface ip<dirección_IP>
store network interface mask<máscara_red>
store network routes defaultroute<dirección_pasarela>
restart network
```

Si el problema aún no se ha resuelto, póngase en contacto con el soporte de Guardium para una intervención manual.

Tema principal: Configuración del sistema Guardium

La máquina virtual Guardium no es accesible desde la red

Si la máquina virtual Guardium no es accesible desde la red, ejecute el inventario de interfaz de red de almacén de mandatos y reinicie el sistema.

Síntomas

Ha implementado un nuevo sistema Guardium como una máquina virtual y ha realizado toda la configuración de red inicial necesaria. Sin embargo, no puede ejecutar ping al sistema utilizando la dirección IP y el sistema no es accesible en la red.

Causas

La dirección MAC asignada a la máquina virtual por el entorno virtual no coincide con la dirección MAC en Guardium.

Entorno

Afecta al recopilador, al agregador y al gestor central.

Diagnóstico del problema

Para diagnosticar el problema, ejecute ping a la dirección IP en una red. Utilice el mandato ping<dirección IP del dispositivo>. Si falla, muestra la dirección MAC del sistema.

1. Inicie sesión como usuario "cli".
2. Ejecute el mandato show network macs para que se muestre la dirección MAC almacenada en la configuración de Guardium.
3. Desde el programa de utilidad de administración de su entorno virtual, compruebe la dirección MAC de la máquina virtual.
    a. Abra la estación de trabajo de VMWare.
    b. Pulse con el botón derecho del ratón en la máquina virtual y seleccione Valores o Propiedades para abrir los Valores de máquina virtual.
    c. Seleccione Adaptador de red en Hardware.
    d. Pulse Avanzado para abrir Valores avanzados del adaptador de red.
    e. Compare la dirección MAC de los pasos 2 y 3.

Resolución del problema

Para resolver el problema, realice los pasos siguientes.

1. Inicie sesión en el sistema Guardium como usuario "cli".
2. Ejecute el mandato store network interface inventory.
3. Especifique `y` para restablecer los NIC.
4. Reinicie el sistema con el mandato restart system.

Tema principal: Configuración del sistema Guardium

SSLv3 está habilitado

Si recibe un aviso de que `SSLv3 está habilitado`, inhabilite SSLv3 para evitar que se aproveche POODLE.

Síntomas

Recibe el aviso siguiente: `SSLv3 está habilitado`.

Causas

SSLv3 contiene una vulnerabilidad de protocolo conocida como POODLE (Padding Oracle On Downgraded Legacy Encryption). Si SSLv3 está habilitado en el sistema, esta vulnerabilidad permite que los atacantes fuercen el cambio de SSL/TLS a SSLv3, averigüen el cifrado e intercepten tráfico de red en texto sin formato. La vulnerabilidad se detalla en National Vulnerability Database como CVE-2014-3566.

Guardium recomienda inhabilitar SSLv3 en todos los sistemas para evitar que se aproveche POODLE, y SSLv3 está inhabilitado de forma predeterminada en los nuevos sistemas Guardium. Sin embargo, los sistemas anteriores y algunos escenarios de actualización pueden dejar SSLv3 habilitado.

Este tema describe cómo comprobar el estado de SSLv3 e inhabilitarlo si es necesario.

Atención: La inhabilitación de SSLv3 puede interrumpir la conectividad entre un Gestor central de Guardium v10 y algunas unidades gestionadas que ejecuten Guardium v9 anterior a GPU 500. Si tiene un entorno mixto con unidades destinadas que ejecutan Guardium v9 anterior a GPU 500, actualice las unidades destinadas a GPU 500 o aplique el parche 9501 antes de inhabilitar SSLv3.

Resolución del problema

1. Verifique el estado de SSLv3 utilizando el mandato de CLI siguiente: `show sslv3`.
    - Si la salida indica `El valor de SSL está inhabilitado`, SSLv3 está inhabilitado. No se requieren pasos adicionales para inhabilitar SSLv3.
    - Si la salida indica `El valor de SSL está habilitado`, SSLv3 está habilitado. Continúe con este procedimiento para inhabilitar SSLv3.
2. Inhabilite SSLv3 utilizando el mandato de CLI siguiente: `store sslv3 off`. La salida del mandato debe ser similar a la siguiente:

```
El valor de SSL actual está habilitado.  Cambiará a inhabilitado.
Reiniciando la GUI
Cambiando al puerto 8443
Desde el puerto 8443
Deteniendo.......
Aceptar
```

3. Verifique que SSLv3 está ahora inhabilitado: `show sslv3`. Ahora la salida debería indicar `El valor de SSL está inhabilitado`.

Tema principal: Configuración del sistema Guardium

Gestión de acceso

- No se puede iniciar sesión en Guardium, salvo como admin o accessmgr
  Si no puede iniciar sesión en la interfaz gráfica de usuario de Guardium, excepto como admin o accessmgr, compruebe los valores de configuración de la autenticación.
- Restablecimiento de la contraseña de accessmgr de Guardium
  Si pierde la contraseña de accessmgr y no puede iniciar sesión, póngase en contacto con el soporte de Guardium.

Tema principal: Problemas y soluciones

No se puede iniciar sesión en Guardium, salvo como admin o accessmgr

Si no puede iniciar sesión en la interfaz gráfica de usuario de Guardium, excepto como admin o accessmgr, compruebe los valores de configuración de la autenticación.

Síntomas

No puede iniciar sesión en Guardium con ningún usuario, salvo admin o accessmgr. Verá un error de nombre de usuario o contraseña no válido a pesar de utilizar el usuario y la contraseña correctos definidos por accessmgr. Recibe el siguiente mensaje de error. `Nombre de usuario y/o contraseña no válidos. Vuelva a especificar sus credenciales.`

Causas

El valor de autenticación no se ha configurado como local.

Entorno

Afecta al recopilador, al agregador y al gestor central.

Resolución del problema

Para resolver el problema, cambie el valor de autenticación a local. Esta acción le permite iniciar sesión con cualquier usuario definido en accessmgr.

Tema principal: Gestión de acceso

Restablecimiento de la contraseña de accessmgr de Guardium

Si pierde la contraseña de accessmgr y no puede iniciar sesión, póngase en contacto con el soporte de Guardium.

Síntomas

Ha perdido la contraseña de accessmgr de Guardium y no puede iniciar sesión en la interfaz gráfica de usuario. La cuenta también se bloquea después de sucesivos intentos fallidos.

Causas

Guardium prohíbe varios intentos fallidos de inicio de sesión.

Entorno

Afecta al recopilador, al agregador y al gestor central.

Resolución del problema

Inicie sesión en la CLI y ejecute el mandato siguiente: support reset-password accessmgr <N> |random.

Puede utilizar <N> o random, donde <N> es un número del rango 10000000 - 99999999. Random genera automáticamente un número del rango de 10000000-99999999. Abra un PMR con el soporte de IBM Guardium y envíe la salida siguiente.

```
G10.ibm.com> support reset-password accessmgr random
Password for accessmgr account have been successfully reset using keyword:<passkey>
Please provide these number to Guardium Customer Service to receive actual account password.
ok
```

Después de recibir la nueva contraseña, desbloquee la cuenta.

1. Utilice el mandato siguiente para desbloquear la cuenta. unlock accessmgr.
2. Inicie sesión como accessmgr y edite los detalles de accessmgr para especificar una contraseña temporal.
3. Vuelva a iniciar sesión con la contraseña temporal.
4. Cuando se le solicite, especifique una nueva contraseña.

Tema principal: Gestión de acceso

Agregación

- No se puede convertir el recopilador de Guardium en agregador
  Si no puede convertir un recopilador de Guardium en un agregador de Gestor central, vuelva a instalar Guardium y seleccione el agregador durante la instalación.
- Un cambio de configuración de Exportación de datos desde la interfaz gráfica de usuario de un sistema gestionado Guardium falla con error
  Si un cambio de configuración de Exportación de datos falla, asegúrese de que la clave secreta compartida sea la misma en el recopilador y el agregador.
- Diferencias entre resultados y el informe del proceso de auditoría
  Si hay diferencias entre los resultados y el informe del proceso de auditoría, compruebe que todos los dispositivos estén establecidos en el mismo huso horario.
- Errores HY000 después de restaurar la configuración en un agregador
  Si recibe errores HY000 después de restaurar la configuración en un agregador, ejecute una importación ficticia.

Tema principal: Problemas y soluciones

No se puede convertir el recopilador de Guardium en agregador

Si no puede convertir un recopilador de Guardium en un agregador de Gestor central, vuelva a instalar Guardium y seleccione el agregador durante la instalación.

Síntomas

Intente convertir un recopilador de Guardium en un agregador con el mandato store unit type manager aggregator.

Sin embargo, el mandato siguiente muestra que el tipo de unidad aún se lista como gestor.

```
> show unit type
Manager
```

Causas

Un recopilador no se puede convertir en un agregador con un mandato de CLI.

Entorno

Afecta a los recopiladores de Guardium.

Resolución del problema

Para convertir un recopilador en un agregador, vuelva a instalar el producto Guardium como el tipo de unidad durante la instalación. Después de instalar el agregador, puede convertirlo en un agregador de gestor central con el mandato store unit type manager.

Obligatoriedad de Gestor central/agregador
: A partir de la versión 9.5 (v9.0 parche 500), la aplicación obligará a que un Gestor central tenga que ser un dispositivo de tipo Agregador. Esto significaría que, a partir de la versión 9.5, sólo los dispositivos de tipo Agregador serán promocionables al dispositivo de Gestor central. Los dispositivos Gestor central existentes antes de la versión 9.5 no están sujetos a este cambio.

Tema principal: Agregación

Un cambio de configuración de Exportación de datos desde la interfaz gráfica de usuario de un sistema gestionado Guardium falla con error

Si un cambio de configuración de Exportación de datos falla, asegúrese de que la clave secreta compartida sea la misma en el recopilador y el agregador.

Síntomas

Intenta guardar nuevos valores para la exportación de datos y recibe un error al pulsar Aplicar para guardar la configuración:

```
Corrija los errores siguientes y vuélvalo a intentar:
No se puede enviar un archivo de datos de prueba a este host con los parámetros proporcionados.
Confirme que el nombre de host o la dirección IP se hayan especificado correctamente, que el
host esté en línea, que el directorio de destino exista y que un usuario determinado pueda
escribir en él, y que la contraseña proporcionada sea correcta para el usuario.
```

Causas

Guardium intenta iniciar sesión con scp en el host de destino con el usuario y la contraseña especificados en la configuración de Exportación de datos. A continuación, Guardium intenta copiar un archivo de prueba en el directorio de destino. El secreto compartido en este sistema no coincide con el secreto compartido en el agregador al que está intentando establecer que exporte este sistema.

Entorno

Afecta a las configuraciones de Guardium, recopilador y agregador.

Resolución del problema

Asegúrese de que la clave secreta compartida sea la misma en el recopilador y en el agregador. Puede utilizar uno de los métodos siguientes:

1. Si sabe el secreto compartido en el agregador, establezca el secreto compartido en el recopilador en el mismo valor. Puede utilizar uno de estos métodos:
   - Desde la CLI: Utilice el mandato store system shared secret para establecer la clave de secreto compartido
   - Desde la interfaz gráfica de usuario: Establezca la clave secreta compartida en Configuración > Sistema > Configuración del sistema.
2. Haga copia de seguridad del secreto compartido actual en el agregador y restáurelo en el recopilador.
   - En el agregador, ejecute el mandato de CLI.

     ```
     aggregator backup keys file <usuario@host:/vía_de_acceso/nombre_archivo>
     Parámetros
     usuario@host:/vía_de_acceso/nombre_archivo
     ```

     Para la operación de transferencia de archivos, especifique un usuario, host y nombre de vía de acceso completo para el archivo de claves de copia de seguridad. El usuario que especifique debe tener autorización para escribir en el directorio especificado.
   - En el recopilador, ejecute este mandato para restaurar la clave de secreto compartido:

     ```
     aggregator restore keys file<usuario@host:/vía_de_acceso/nombre_archivo>
     ```
3. Restablezca el secreto compartido para ambos dispositivos de manera que sea el mismo.
   Nota: Si cambia el secreto compartido para el agregador, debe restablecer el secreto compartido para todos los demás sistemas Guardium que exportan a él.

Tema principal: Agregación

Diferencias entre resultados y el informe del proceso de auditoría

Si hay diferencias entre los resultados y el informe del proceso de auditoría, compruebe que todos los dispositivos estén establecidos en el mismo huso horario.

Síntomas

Puede establecer un informe para que se ejecute en el agregador como parte de un proceso de auditoría con parámetros de tiempo, por ejemplo, Inicio del último día y Final del último día. Cuando consulte los resultados de ese informe, las primeras indicaciones de hora estarán siempre establecidas en una hora posterior a las 00.00, por ejemplo, 02.00. Además, las últimas indicaciones de hora estarán siempre establecidas en una hora anterior a las 23.59, por ejemplo, 21.59. No obstante, cuando ejecuta el informe interactivamente, las indicaciones de hora se muestran de la forma esperada.

Causas

Es posible que el recopilador y el agregador no tengan el mismo huso horario.

Entorno

Afecta al agregador.

Diagnóstico del problema

Compruebe que todos los dispositivos estén establecidos en el mismo huso horario. Utilice el mandato siguiente. `show system clock timezone.`

Resolución del problema

Si el recopilador y el agregador no están establecidos en el mismo huso horario, configure el huso horario de los dispositivos con la CLI.

```
store system clock timezone list
store system clock timezone <huso_horario>
```

Compruebe que la hora sea correcta en el dispositivo con los mandatos siguientes.

```
show system clock datetime
store system clock datetime
```

El huso horario también se puede sincronizar utilizando un servidor NTP con los mandatos siguientes.

```
show system ntp all
store system ntp state
store system ntp server
```

Tema principal: Agregación

Errores HY000 después de restaurar la configuración en un agregador

Si recibe errores HY000 después de restaurar la configuración en un agregador, ejecute una importación ficticia.

Síntomas

Cuando restaura la configuración de un agregador o del Gestor central, recibe uno de estos mensajes, o ambos.

```
ERROR 1031 (HY000) en la línea 1: el motor de almacenamiento de tabla para 'GUARD_USER_ACTIVITY_AUDIT' no tiene esta opción
ERROR 1031 (HY000) en la línea 1: el motor de almacenamiento de tabla para 'AGGREGATOR_ACTIVITY_LOG' no tiene esta opción
```

Causas

Esta condición de error se puede producir si hay una discrepancia temporal en las bases de datos internas.

Entorno

Afecta al recopilador y al agregador.

Resolución del problema

Para resolver el problema, ejecute una importación ficticia.

Tema principal: Agregación

Gestión central

- Un usuario está inhabilitado en una unidad gestionada de Guardium, pero se muestra como habilitado en el Gestor central
  Si un usuario está inhabilitado en una unidad gestionada de Guardium, pero se muestra como habilitado en el Gestor central, ejecute la sincronización de usuarios del portal.
- El Gestor central no reconoce la nueva versión de las unidades actualizadas
  Si el Gestor central no reconoce la nueva versión de las unidades actualizadas, seleccione las unidades actualizadas y renueve la página.
- Las tareas planificadas no se activan a la hora planificada
  Si las tareas planificadas no se activan a la hora planificada, planifique la hora de importación para que se ejecuten después de la sincronización de usuarios del portal.
- Excepción de Torque en la vista Gestión central de la interfaz gráfica de usuario
  Si hay una excepción de Torque en Gestión central, suprima el grupo personalizado y cree un grupo nuevo.

Tema principal: Problemas y soluciones

Un usuario está inhabilitado en una unidad gestionada de Guardium, pero se muestra como habilitado en el Gestor central

Si un usuario está inhabilitado en una unidad gestionada de Guardium, pero se muestra como habilitado en el Gestor central, ejecute la sincronización de usuarios del portal.

Síntomas

Un usuario está inhabilitado en la unidad gestionada. La cuenta del usuario se ha vuelto a habilitar en el Gestor central pero el usuario aún se muestra como inhabilitado en la unidad gestionada. La cuenta del usuario se muestra como habilitada en el Gestor central.

Causas

La cuenta del usuario en el Gestor central no está sincronizada con la unidad gestionada.

Entorno

Podría afectar a una combinación de Gestor central, recopilador o agregador.

Resolución del problema

Para sincronizar el estado de usuario actual entre el Gestor central y la unidad gestionada, ejecute una sincronización de usuarios del portal.

1. Inicie sesión en el Gestor central como usuario de administración.
2. Pulse Gestionar > Gestión central > Sincronización de usuarios del portal para abrir la gestionar la Sincronización de usuarios del portal.
3. Pulse Ejecutar una vez ahora.

Si la cuenta del usuario entre la unidad gestionada y el Gestor central no está todavía sincronizada, póngase en contacto con el soporte técnico de IBM Guardium para obtener ayuda.

Tema principal: Gestión central

El Gestor central no reconoce la nueva versión de las unidades actualizadas

Si el Gestor central no reconoce la nueva versión de las unidades actualizadas, seleccione las unidades actualizadas y renueve la página.

Síntomas

Es posible que el Gestor central no reconozca inmediatamente la nueva versión de un agregador o recopilador que gestiona. Si se envía un parche desde el Gestor central, lo que requiere la nueva versión, se puede generar un error que muestra que la unidad sigue estando en la versión anterior.

La versión anterior de la unidad gestionada aún aparece en la vista Gestión central de la interfaz gráfica de usuario. La unidad tiene tiempos de ping en dicha vista, lo que implica una buena comunicación entre el Gestor central y las unidades gestionadas.

Causas

Debe renovarse la interfaz gráfica de usuario para extraer la información de la nueva versión.

Entorno

Afecta al Gestor central de Guardium.

Resolución del problema

En la vista Gestión central de la interfaz gráfica de usuario, seleccione las unidades actualizadas y pulse Renovar. Esta acción extrae la información de la nueva versión de las unidades.

Tema principal: Gestión central

Las tareas planificadas no se activan a la hora planificada

Si las tareas planificadas no se activan a la hora planificada, planifique la hora de importación para que se ejecuten después de la sincronización de usuarios del portal.

Síntomas

La importación falla y el usuario recibe el mensaje siguiente en agg_progress.log.

```
* 05/20 04:00:01 --- Import cannot start
(guard_agg|turbine_backup.sh|restore_from_file.pl already running)
* 05/20 20:00:46 --- Merge cannot start - aggregation still active
```

Causas

Hay un conflicto con la sincronización de usuarios del portal del Gestor central.

Entorno

Afecta al agregador.

Diagnóstico del problema

Averigüe qué tarea se está ejecutando en segundo plano. Pulse Informes > Informes operativos de Guardium > Registro de agregación/archivado para abrir el Registro de agregación/archivado.

Resolución del problema

Para resolver el problema, planifique la hora de importación para que se ejecute después de la sincronización de usuarios del portal. Ejecute la sincronización de usuarios del portal cada hora y la hora de importación 30 minutos después de dicha hora.

Tema principal: Gestión central

Excepción de Torque en la vista Gestión central de la interfaz gráfica de usuario

Si hay una excepción de Torque en Gestión central, suprima el grupo personalizado y cree un grupo nuevo.

Síntomas

Cuando se selecciona un determinado grupo personalizado en la vista Gestión central de la interfaz gráfica de usuario de Guardium, aparece un error en lugar de las unidades gestionadas del grupo.

```
org.apache.torque.TorqueException: Failed to select one and only one row.
```

Cuando aparece la excepción, se muestra para cualquier grupo o vista en el separador Gestión central. La excepción incluso aparece para grupos que funcionaban anteriormente, hasta que cerró la sesión en la interfaz gráfica de usuario y volvió a iniciarla.

Causas

Esta excepción de Torque puede producirse si una de las unidades gestionadas del grupo se ha eliminado de la unidad gestionada en vez de eliminarse del gestor central.

Entorno

Afecta al Gestor central de Guardium.

Resolución del problema

Suprima el grupo personalizado y cree un grupo nuevo que contenga los mismos miembros.

Tema principal: Gestión central

S-TAP y otros agentes

- Error de AIX 6.1 al instalar o actualizar el S-TAP dex IBM Security Guardium
  Si el sistema operativo falla al instalar o actualizar S-TAP de Guardium en AIX 6.1, aplique los fixpacks de AIX 6.1.
- Error al abrir el área de memoria compartida cuando se configura COMM_EXIT_LIST de Guardium para DB2
  Si recibe un mensaje de error cuando configura COMM_EXIT_LIST de Guardium, autorice al propietario de la instancia de DB2 con el mandato guardctl.
- Guardium no puede recopilar el tráfico de la memoria compartida de Informix
  Si Guardium no puede recopilar el tráfico de memoria compartida de Informix, compruebe la configuración del motor de inspección.
- Uso elevado de CPU y E/S en el host STAP de Guardium
  Si observa un uso elevado de E/S o de CPU, revise la configuración de todos los motores de inspección.
- Falta información del paquete de inicio de sesión
  Si falta información en el paquete de inicio de sesión, recopile el rastreo de depuración y el rastreo de slon de S-TAP.
- El proceso nanny interrumpe sniffer
  Si el proceso nanny interrumpe sniffer, es posible que tenga demasiado tráfico de entrada.
- Sniffer no se puede conectar a UNIX S-TAP
- S-TAP no se puede iniciar
  Si un S-TAP no puede iniciarse, es posible que su tamaño de almacenamiento intermedio sea demasiado grande.
- S-TAP no se inicia automáticamente en Linux
  Si el agente S-TAP para DB2 u Oracle no se inicia automáticamente en Linux, compruebe el directorio /etc/event.d/.
- S-TAP devuelve "Not FIPS 140-2 complaint"
  Si recibe un error acerca de FIPS 140-2, cambie la configuración mediante la página Control de S-TAP.
- El módulo de kernel K-TAP sigue presente tras la desinstalación de S-TAP
  Si el módulo de kernel K-TAP sigue presente después de la desinstalación de S-TAP, elimínelo manualmente.
- S-TAP de UNIX no puede leer más de 16 motores de inspección
  Si S-TAP de UNIX no puede leer más de 16 motores de inspección, cambie los parámetros de puerto de escucha o utilice PCAP.
- El servicio S-TAP de Windows se cuelga al iniciarse con el ID de error 1000
  Si el S-TAP se cuelga con el ID de error 1000, compruebe el parámetro SOFTWARE_TAP_IP en el archivo de configuración guard_tap_ini.
- S-TAP de z/OS no se muestra activo en el sistema Guardium
  Si S-TAP de z/OS no se muestra activo en el sistema Guardium, reinicie el núcleo de inspección.

Tema principal: Problemas y soluciones

Error de AIX 6.1 al instalar o actualizar el S-TAP dex IBM Security Guardium

Si el sistema operativo falla al instalar o actualizar S-TAP de Guardium en AIX 6.1, aplique los fixpacks de AIX 6.1.

Síntomas

El sistema operativo falla al instalar o actualizar S-TAP de Guardium en AIX 6.1. El volcado de memoria del bloqueo de AIX muestra el siguiente rastreo de pila.

```
Error ID: DD11B4AF Resource Name: SYSPROC
Detail Data: 00007FFFFFFFD080 0000000000473260
0000000000020000 8000000000029032

Symptom Information:
Crash Location: [0000000000473260] execvex_common+1880
Component: COMP Exception Type: 131

Stack Trace:
[0000000000473260] execvex_common+1880
[000000000047744C] execve+A8
[F1000000C083E84C] my_execve+424
```

Causas

Este bloqueo es un problema conocido en AIX versión 6.1 debido a un bloqueo del sistema en la vía de acceso de código execvex_common.

Entorno

Afecta a cualquier S-TAP que se instale en el sistema operativo AIX 6.1.

Resolución del problema

Para aplicar el fixpack de AIX 6.1 6100-08-04 y resolver el problema, consulte http://www-01.ibm.com/support/docview.wss?uid=isg1IV50179

Tema principal: S-TAP y otros agentes

Error al abrir el área de memoria compartida cuando se configura COMM_EXIT_LIST de Guardium para DB2

Si recibe un mensaje de error cuando configura COMM_EXIT_LIST de Guardium, autorice al propietario de la instancia de DB2 con el mandato guardctl.

Síntomas

Después de configurar DB2 COMM_EXIT_LIST para utilizar Guardium libguard y reiniciar el servidor DB2, obtendrá el error siguiente en el registro diag de DB2.

```
2013-06-28-11.41.12.306169-300 E870950E486 LEVEL: Severe
PID : 15764 TID : 139905833363200 PROC : db2sysc 0
INSTANCE: db2001 NODE : 000
APPHDL : 0-16
HOSTNAME: dbhost1
EDUID : 54 EDUNAME: db2agent () 0
FUNCTION: DB2 UDB, DRDA Communication Manager, sqljcCommexitLogMessage,
probe:234
DATA #1 : String with size, 91 bytes
WARNING: Shmem_access /.guard_writer0 failed Error opening shared memory area errno=2 err=8
```

Causas

El siguiente mensaje indica que la biblioteca de Guardium no ha podido crear el dispositivo de memoria compartida que necesita.

```
Shmem_access /.guard_writer0 failed
Error opening shared memory area
errno=2
err=8
```

El propietario de la instancia de DB2 se debe añadir como un usuario autorizado mediante el mandato guardctl.

Entorno

Recopiladores de Guardium que utilizan DB2 Exit (Versión 10) Afecta a la integración con S-TAP.

Resolución del problema

El propietario de la instancia de DB2 se debe añadir como un usuario autorizado mediante el mandato guardctl.

1. Detenga la instancia de DB2.
2. Autorice al propietario de la instancia de DB2.
3. Inicie la instancia de DB2.

Si no se ha instalado Guardium Installation Manager (GIM), autorice al propietario de la instancia de DB2 con el mandato siguiente.

```
<dir_inst_guardium>/bin/guardctl authorize-user<propietario_inst_db2>
```

Si está instalado Guardium Installation Manager (GIM), autorice al propietario de la instancia de DB2 con el mandato siguiente.

```
<dir_inst_guardium>/modules/ATAP/current/files/bin/guardctl authorize-user<propietario_inst_db2>
```

Por ejemplo, si el propietario de la instancia de DB2 es db2001 y GIM está instalado en /usr/local/guardium, el mandato es `/usr/local/gim/modules/ATAP/current/files/bin/guardctl authorize-user db2001`.

Tema principal: S-TAP y otros agentes

Guardium no puede recopilar el tráfico de la memoria compartida de Informix

Si Guardium no puede recopilar el tráfico de memoria compartida de Informix, compruebe la configuración del motor de inspección.

Síntomas

S-TAP de Guardium no recopila el tráfico de memoria compartida de Informix.

Causas

El motor de inspección no está configurado correctamente.

Entorno

Afecta a cualquier recopilación de S-TAP de cualquier sistema Informix.

Resolución del problema

Compruebe la configuración del motor de inspección en Gestionar > Supervisión de actividad > Control de S-TAP. Asegúrese de que el valor del campo Nombre de proceso coincida con el resultado del mandato siguiente en el servidor de base de datos.

```
ls -lrt /INFORMIXTMP/.inf.*
```

Informix: /INFORMIXTMP/.inf.sqlexec Se aplica a todas las plataformas Informix salvo Linux. Para Informix con Linux, ejemplo: /home/informix11/bin/oninit

Para que este mandato devuelva un valor, Informix debe estar en ejecución.

Para servidores Linux, A-TAP debe estar configurado para recopilar cualquier tráfico de memoria compartida. Establezca el valor en el mismo valor que el del parámetro --db-info en la configuración de A-TAP antes de activar A-TAP.

Tema principal: S-TAP y otros agentes

Uso elevado de CPU y E/S en el host STAP de Guardium

Si observa un uso elevado de E/S o de CPU, revise la configuración de todos los motores de inspección.

Síntomas

El usuario observa un uso elevado de E/S o de CPU por parte del proceso S-TAP de Guardium.

Causas

Los elementos siguientes son causas habituales.

1. Un error en la configuración de uno de los motores de inspección. Si hay errores en un motor de inspección, el proceso S-TAP se reinicia con frecuencia o intenta volver a conectarse al motor de inspección repetidamente.
2. La parte de K-TAP del S-TAP envía información de conexión junto con una solicitud de confirmación al S-TAP. Este paso causa retardos.
3. Se utiliza ORACLE RAC, pero el parámetro unix_domain_socket_marker no se ha establecido en el archivo de configuración de S-TAP para evitar que se supervisen cantidades potencialmente grandes de tráfico de RAC de Oracle.
4. La característica Cadena de ID de usuario (Cadena de UID) está habilitada, por ejemplo, parameter hunter_trace= 1 en el archivo de configuración de S-TAP. Se utiliza rastreo Hunter para cadena de UID, que puede consumir considerables recursos de CPU para S-TAP.
5. El cortafuegos está habilitado (firewall_installed= 1). Este cortafuegos obliga a S-TAP a solicitar veredictos para cada nueva sesión que se observa que puede afectar al rendimiento de S-TAP.

Entorno

S-TAP instalado en AIX

Resolución del problema

Según la causa, realice las acciones correspondientes.

1. Revise la configuración de todos los motores de inspección y asegúrese de que no haya errores en ninguno de los parámetros. Por ejemplo, asegúrese de que el directorio, el ejecutable, los puertos y los demás parámetros de base de datos aplicables al motor de la inspección se hayan establecido correctamente sin errores ortográficos o valores erróneos.
2. Establezca el parámetro de configuración de S-TAP ktap_fast_tcp_verdict en 1 (ktap_fast_tcp_veredic=1 en el archivo de configuración guard_tap.ini) y reinicie el S-TAP. Estos son los valores posibles.

   ktap_fast_tcp_verdict= 0: KTAP confirma que la sesión es la conexión de base de datos que el motor de inspección ha configurado comprobando los puertos y las IP.

   ktap_fast_tcp_verdict= 1: KTAP no envía la solicitud a S-TAP mientras los puertos de la sesión están en el rango.

3. Inhabilite la característica Cadena de UID si no es necesaria estableciendo hunter_trace= 0 y reiniciando el S-TAP.
4. Establezca firewall_installed=0 si no se necesita SGATE y reinicie el S-TAP.

Tema principal: S-TAP y otros agentes

Falta información del paquete de inicio de sesión

Si falta información en el paquete de inicio de sesión, recopile el rastreo de depuración y el rastreo de slon de S-TAP.

Síntomas

Puede encontrar problemas en Guardium relativos a información que falta en el paquete de inicio de sesión como, por ejemplo, el nombre de usuario de base de datos, el programa fuente o el nombre de base de datos.

Causas

Cuando la sesión es demasiado corta, podría faltar información en los paquetes de inicio de sesión.

Entorno

Afecta al recopilador de Guardium.

Resolución del problema

Recopile el rastreo de depuración de S-TAP en el servidor de base de datos donde está instalado el S-TAP de Guardium y el rastreo de slon en el recopilador.

Consulte las notas técnicas en la sección de URL relacionados para obtener detalles sobre cómo recopilar cada uno de estos rastreos.

1. Ejecute ambos rastreos al mismo tiempo.
2. Genere una nueva sesión de base de datos que recree el problema mientras se ejecuten ambos rastreos. Los paquetes de inicio de sesión sólo se envían cuando la conexión de base de datos está abierta.
3. Añada el inicio de sesión, el puerto de cliente y el puerto de servidor al informe existente. Renueve el informe después de volver a crear el problema con la nueva conexión.
4. Confirme que los rastreos se están ejecutando durante la sesión comprobando el inicio de sesión.
5. Deje abierta la sesión durante 5 minutos como mínimo para permitir que el sniffer analice los paquetes de inicio de sesión.
6. Envíe la sesión con los campos que faltan. Indique el nombre de la aplicación que ha utilizado para generar la sesión, el nombre de base de datos, el usuario BD con el que se ha conectado, el tipo de conexión, la sentencia SQL y cualquier otra información pertinente.
7. Recopile el archivo de rastreo de depuración de S-TAP en el servidor de base de datos, el rastreo de slon en el recopilador de Guardium y el sniffer actual Must Gather.

Tema principal: S-TAP y otros agentes

El proceso nanny interrumpe sniffer

Si el proceso nanny interrumpe sniffer, es posible que tenga demasiado tráfico de entrada.

Síntomas

Se notifica un mensaje similar al siguiente una o más veces en el registro (los mensajes) del sistema Guardium o en alertas:

```
Nanny process error condition. The nanny process killed the sniffer. VmData was número and was over the limit.
```

Causas

El uso de memoria de sniffer ha alcanzado más del 90 % de la memoria disponible y el proceso nanny lo ha reiniciado, lo que es el comportamiento previsto del producto.

Entorno

Recopilador de Guardium

Resolución del problema

Si observa este mensaje con frecuencia, llega demasiado tráfico al sistema Guardium. Reduzca el tráfico a este sistema Guardium para resolver este mensaje. Por ejemplo, puede mover algunos STAP a un recopilador con menos carga, ignorar algún tráfico en la política, o implementar el equilibrio de carga para distribuir el tráfico entre más de un recopilador.

Si se observa el mensaje esporádicamente, probablemente se trata de un pico de tráfico. Para resolver el mensaje, identifique la razón del pico y evite el desencadenante. Por ejemplo, puede revisar qué procesos se ejecutaban en ese momento e identificar los que generaban más tráfico. Si este mensaje siempre coincide con un proceso o procesos determinados en ejecución, reduzca el tráfico simultáneo en ese momento. Por ejemplo, puede mover el proceso más pesado para que se ejecute en otro momento, o ignorar parte de ese tráfico mediante una política.

Tema principal: S-TAP y otros agentes

Sniffer no se puede conectar a UNIX S-TAP

Síntomas

Cuando especifica un número diferente de hebras, por ejemplo, 20, mediante el mandato snif -t 20, el sniffer no se puede conectar al S-TAP de UNIX. En la consola de la GUI, el estado del S-TAP es inactivo.

Causas

De forma predeterminada, el sniffer se inicia con seis hebras. Cuando el número de hebras supera la limitación, el sniffer no se puede conectar al S-TAP de UNIX debido a un comportamiento indefinido.

Entorno

Afecta al S-TAP de UNIX.

Resolución del problema

Reduzca el número de hebras para asegurarse de que la conexión se puede establecer correctamente.

Tema principal: S-TAP y otros agentes

S-TAP no se puede iniciar

Si un S-TAP no puede iniciarse, es posible que su tamaño de almacenamiento intermedio sea demasiado grande.

Síntomas

El S-TAP no puede iniciarse y emite los mensajes siguientes:

```
mmap: Not enough space
Can't initialize: Can't mmap buffer file /tmp/stapbuf/192.168.100.107.0.buf
Error Initializing: Stap cannot initialize SQLGuard queue
```

Causas

El S-TAP no puede asignar memoria suficiente para que se corresponda con el archivo de almacenamiento intermedio.

Resolución del problema

Reduzca el tamaño del archivo de almacenamiento intermedio para el S-TAP. El tamaño se especifica en el parámetro buffer_file_size en el archivo guard_tap.ini.

Tema principal: S-TAP y otros agentes

S-TAP no se inicia automáticamente en Linux

Si el agente S-TAP para DB2 u Oracle no se inicia automáticamente en Linux, compruebe el directorio /etc/event.d/.

Síntomas

El proceso S-TAP no se inicia automáticamente en Linux incluso aunque el archivo /etc/inittab muestre una entrada U-TAP correcta.

Causas

Diversas distribuciones de Linux como por ejemplo RedHat 6 han dejado de utilizar el daemon de inicialización tradicional que utiliza el archivo etc/inittab. Lo han sustituido por un proceso init denominado upstart. Upstart utiliza los directorios /etc/event.d y /etc/init para el inicio, la detención y la regeneración automatizados de procesos como por ejemplo U-TAP.

El instalador S-TAP ahora comprueba la existencia del directorio /etc/event.d. Si existe, se crean entradas en /etc/init para que las utilice upstart. Si no existe, se crean entradas en /etc/inittab para que las utilice el daemon de inicialización tradicional.

Si falta /etc/event.d por cualquier motivo en un sistema con upstart, se llena en su lugar el archivo inittab. El proceso S-TAP no se inicia ni se vuelve a generar cuando es necesario.

Entorno

Afecta a los S-TAP en ejecución en Linux.

Resolución del problema

Compruebe la existencia del directorio /etc/event.d/.

Si el directorio /etc/event.d/ no existe, complete los pasos siguientes para resolver la situación.

1. Desinstale la instalación S-TAP existente.
2. Cree el directorio /etc/event.d como usuario root (mkdir /etc/event.d).
3. Instale el S-TAP.

Tema principal: S-TAP y otros agentes

S-TAP devuelve "Not FIPS 140-2 complaint"

Si recibe un error acerca de FIPS 140-2, cambie la configuración mediante la página Control de S-TAP.

Síntomas

Soportado: - Solaris X86 - Linux x86/64 - Linux x86/32 - Linux S390X - Linux IA64 No soportado: - Solaris SPARC - AIX PowerPC - HPUX RISC - HPUX IA64 - Linux PowerPC

Ve el siguiente mensaje en el registro de sucesos de S-TAP.

```
LOG_ERR: Not FIPS 140-2 compliant - use_tls=0 failover_tls=1.
```

Causas

FIPS 140-2 es un estándar de seguridad del gobierno de Estados Unidos para módulos criptográficos. Si ve este mensaje, indica que la configuración de S-TAP no cumple los requisitos del gobierno.

Nota: Este mensaje no indica que haya un error en el S-TAP.

Entorno

Afecta al S-TAP de Guardium.

Soportado: Solaris X86; Linux x86/64; Linux x86/32; Linux S390X; Linux IA64

No soportado: Solaris SPARC; AIX PowerPC; HPUX RISC; HPUX IA64; Linux PowerPC

Resolución del problema

Para habilitar el cumplimiento de FIPS, el archivo guard_tap.ini debe tener los valores siguientes.

```
use_tls=1
failover_tls=0
```

Cualquier otra combinación desactiva la modalidad FIPS y da como resultado un mensaje de error.

Puede cambiar la configuración utilizando uno de los métodos siguientes.

1. Pulse Gestionar > Supervisión de actividad > Control de S-TAP.
2. Modifique la sección de detalles para el S-TAP pertinente y utilice los recuadros de selección TLS.
3. Reinicie el S-TAP.

También puede editar directamente el archivo guard_tap.ini en el servidor de BD y reiniciar el S-TAP.

Tema principal: S-TAP y otros agentes

El módulo de kernel K-TAP sigue presente tras la desinstalación de S-TAP

Si el módulo de kernel K-TAP sigue presente después de la desinstalación de S-TAP, elimínelo manualmente.

Síntomas

El módulo de kernel K-TAP sigue presente tras la desinstalación de S-TAP en un servidor Solaris.

Causas

El servidor no se ha reiniciado correctamente para eliminar el módulo de kernel K-TAP en servidores Solaris.

Entorno

Afecta al servidor Solaris tras la desinstalación de S-TAP.

Diagnóstico del problema

Compruebe el servidor Solaris ejecutando las opciones modinfo | grep ktap y ls -al /dev/*tap *.

Resolución del problema

Elimine manualmente el kernel K-TAP con los pasos siguientes.

1. Compruebe que /etc/init.d/upguard se ha eliminado.
2. Elimine /kernel/drv/sparcv9/ktap* y /kernel/drv/ktap*.
3. Ejecute modinfo | grep ktap para obtener el nombre del controlador cargado.
4. A continuación, ejecute rem_drv <controlador cargado>. Por ejemplo: `rem_drv ktap_36821`.
5. Elimine /dev/ktap* y `/dev/guard_ktap`.
6. Reinicie el servidor.
7. Ejecute modinfo | grep ktap para asegurarse de que el controlador ya no está cargado.
8. Elimine las entradas GIM y gsvr de /etc/inittab (sólo si está utilizando sólo GIM).
9. Elimine manualmente los archivos restantes en /usr/local/guardium.

Tema principal: S-TAP y otros agentes

S-TAP de UNIX no puede leer más de 16 motores de inspección

Si S-TAP de UNIX no puede leer más de 16 motores de inspección, cambie los parámetros de puerto de escucha o utilice PCAP.

Síntomas

S-TAP de UNIX sólo lee las primeras 16 definiciones de `port_range` en los valores de motor de inspección.

Causas

Por diseño, K-TAP sólo puede leer 16 definiciones de `port_range`.

Entorno

Afecta a S-TAP de UNIX que utiliza K-TAP y define más de 16 motores de inspección.

Resolución del problema

Utilice los parámetros `port_range_start` y `port_range_end` para incluir todos los puertos necesarios en la definición del primer motor de inspección. Esta acción intercepta todo el tráfico del rango de puertos especificado. Si necesita ignorar algunos puertos en el rango, puede definir una política para ignorar los puertos de servidor innecesarios.

En el ejemplo siguiente se definen los puertos de escucha 50000-50020 como puertos de destino que se van a supervisar.

```
[DB_0]
port_range_end=50020
port_range_start=50000
```

De lo contrario, utilice las conexiones PCAP para TCP estableciendo `ktap_local_tcp=1` y `devices=<nombre_dispositivo>`.

```
[TAP]
ktap_local_tcp=1
devices=<Nombre de dispositivo de red>
```

Tema principal: S-TAP y otros agentes

El servicio S-TAP de Windows se cuelga al iniciarse con el ID de error 1000

Si el S-TAP se cuelga con el ID de error 1000, compruebe el parámetro SOFTWARE_TAP_IP en el archivo de configuración guard_tap_ini.

Síntomas

El S-TAP en un servidor Windows no se inicia. El registro de sucesos de Windows muestra errores del S-TAP de Guardium con el ID de suceso 1000.

```
Nombre de registro:      Aplicación
Origen:        Error de aplicación
ID de evento:  1000
Categoría de la tarea: (100)
Nivel:         Error
Palabras clave:  Classic
Descripción:
Nombre de la aplicación con errores: guardium_stapr.exe, versión: 9.0.0.0
Código de excepción: 0x40000015
```

Causas

S-TAP no se puede conectar al sistema Windows porque se ha especificado el SOFTWARE_TAP_IP incorrecto en el archivo guard_tap.ini.

Entorno

Afecta a cualquier S-TAP de Guardium para Windows.

Resolución del problema

Asegúrese de que el parámetro `SOFTWARE_TAP_IP` del archivo de configuración guard_tap.ini coincida con la dirección IP correcta del servidor de Windows. Este parámetro se pasa en la CLI de instalación o en los parámetros de IBM Guardium Installation Manager (GIM).

Tema principal: S-TAP y otros agentes

S-TAP de z/OS no se muestra activo en el sistema Guardium

Si S-TAP de z/OS no se muestra activo en el sistema Guardium, reinicie el núcleo de inspección.

Síntomas

S-TAP de z/OS no se puede mostrar activo en el sistema Guardium después de iniciarlo por primera vez. La política se ha configurado correctamente con un perfil de recopilación de DB2 o IMS y se ha instalado. El S-TAP de z/OS se ha configurado correctamente para utilizar el puerto 16022. Todos los mensajes del sistema principal indican conectividad.

Causas

Si el recopilador no se ha utilizado de forma activa como un recopilador desde que se compiló y configuró, parece que el sniffer excede el tiempo de espera del puerto 16022.

Entorno

Afecta a z/OS.

Resolución del problema

Reinicie el núcleo de inspección utilizando el mandato de CLI restart inspection-core.

Tema principal: S-TAP y otros agentes

GIM

- Error al instalar Guardium Installation Manager (GIM)
  Si GIM no se instala correctamente, cree el directorio manualmente.
- El servicio Guardium Installation Manager (GIM) no se inicia en Windows
  Si el servicio Guardium Installation Manager (GIM) no se inicia en Windows, vuelva a instalar GIM en una carpeta que esté reservada para aplicaciones de 32 bits.

Tema principal: Problemas y soluciones

Error al instalar Guardium Installation Manager (GIM)

Si GIM no se instala correctamente, cree el directorio manualmente.

Síntomas

Cuando intenta instalar Guardium Installation Manager (GIM) en RHEL6, ve el mensaje de error siguiente.

```
cp: cannot stat `/usr/local/GIM/modules/central_logger.log': No such file or directory Installation failed
```

Causas

Diversas distribuciones de Linux como por ejemplo RedHat 6 han dejado de utilizar el daemon de inicialización tradicional que utiliza el archivo etc/inittab. Lo han sustituido por un proceso init denominado Upstart. Upstart utiliza los directorios /etc/event.d y /etc/init para el inicio, la detención y la regeneración automatizados de procesos.

Entorno

Afecta a Guardium Installation Manager (GIM).

Resolución del problema

Para arreglar el problema, realice los pasos siguientes.

- Elimine la instalación parcial de GIM.
- Cree el directorio /etc/event.d manualmente con el mandato mkdir /etc/event.d
- Ejecute el instalador de GIM.

Tema principal: GIM

El servicio Guardium Installation Manager (GIM) no se inicia en Windows

Si el servicio Guardium Installation Manager (GIM) no se inicia en Windows, vuelva a instalar GIM en una carpeta que esté reservada para aplicaciones de 32 bits.

Síntomas

Cuando ha instalado correctamente Guardium Installation Manager (GIM) en Windows, observa que el servicio no se ejecuta.

Causas

GIM es una aplicación de 32 bits. Si utiliza Windows de 64 bits, GIM podría instalarse en Program Files y no en Program Files(x86).

Entorno

Afecta a GIM.

Resolución del problema

Instale GIM en Program Files(x86) ya que es una carpeta de Windows reservada para aplicaciones de 32 bits.

Tema principal: GIM

Actividad de archivos

- La actividad de archivos no se registra en los informes o panel de control de investigación
- La actividad de archivos del disco extraíble no se registra en el panel de control de investigación
- La actividad de archivos aparece en los informes pero no en el panel de control de investigación
- Faltan algunos archivos de los resultados de clasificación
- Resultados de descubrimiento parcial de archivos (titularidad) en informes y en el panel de control de investigación
  Los informes y el panel de control de investigación no muestran los resultados de descubrimiento completo (titularidad).
- Faltan resultados de clasificación de archivos en los informes y el panel de control de investigación
- El paquete de FAM no se puede instalar
  Después de instalar el cliente de GIM, la instalación del paquete de FAM falla.

Tema principal: Problemas y soluciones

La actividad de archivos no se registra en los informes o panel de control de investigación

Síntomas

No hay actividad de archivos registrada en los informes o el panel de control de investigación como, por ejemplo: Actividades de archivos, Titularidad de archivos, Recuento de archivos de actividad por cliente, Recuento de archivos de actividad por servidor, Recuento de archivos de actividad por usuario, Archivos con privilegios

Resolución del problema

Compruebe lo siguiente:

- Verifique que la licencia de FAM está instalada y que el S-TAP esté activo
- Asegúrese de que no haya iniciado sesión como root en el servidor de archivos para las actividades. De forma predeterminada, las actividades de root (UID0) no se registran.
- En Linux/AIX, compruebe la vía de acceso de archivo especificada en la regla de política. Por ejemplo, /testdir/ supervisa un archivo denominado testdir y no los archivos en un directorio testdir. Especifique /testdir/* para supervisar los archivos del directorio testdir.
- En Windows, si utiliza dominios y la regla de política especifica un usuario, asegúrese de que se haya especificado el dominio. Por ejemplo, svldev\Maryjane en lugar de solo Maryjane.

Tema principal: Resolución de problemas de la actividad de archivos

La actividad de archivos del disco extraíble no se registra en el panel de control de investigación

Síntomas

La actividad de archivos del disco extraíble no se registra en el panel de control de investigación

Entorno

FAM_SCAN_EXCLUDE_REMOTE_DIRECTORIES está establecido en true

Resolución del problema

Instale la política de supervisión de actividad de archivos *antes* de montar el disco extraíble.
Tema principal: Resolución de problemas de la actividad de archivos

La actividad de archivos aparece en los informes pero no en el panel de control de investigación

Síntomas

Verá la actividad de archivos en los informes predefinidos, pero no en el panel de control de investigación.

Resolución del problema

Verifique la configuración que utiliza la API Guard:

- Para enviar datos rastreados a una búsqueda rápida: grdapi enable_fam_crawler activity_schedule_interval= 2 activity_schedule_units=MINUTE entitlement_schedule_intervals=10 entitlement_schedule_units=MINUTE
- Para habilitar la búsqueda rápida (con la opción de incluir también las infracciones): grdapi enable_quick_search includeViolations = true schedule_interval= 2 schedule_units=MINUTE

Tema principal: Resolución de problemas de la actividad de archivos

Faltan algunos archivos de los resultados de clasificación

Síntomas

Faltan algunos archivos de los resultados de clasificación.

Causas

Los siguientes tipos de archivo *no* están soportados para la clasificación: DAT, JPG, JPEG, GIF, TIF, TIFF, BMP, WAV, MOV, MP3, MP4, AVI, MPG, WMA, WMV, P7S, XFDL, XFD, FRM, JAR

Tema principal: Resolución de problemas de la actividad de archivos

Resultados de descubrimiento parcial de archivos (titularidad) en informes y en el panel de control de investigación

Los informes y el panel de control de investigación no muestran los resultados de descubrimiento completo (titularidad).

Síntomas

Los resultados de descubrimiento (titularidad) que aparecen en los informes y en el panel de control de investigación están incompletos. Los resultados de algunos archivos no aparecen.

Resolución del problema

Verifique que los tipos de documento y las ubicaciones están incluidos en las configuraciones de GIM para el descubrimiento. Compruebe los siguientes parámetros de configuración de GIM:

- FAM_SCAN_EXCLUDE_FILES
- FAM_SCAN_EXCLUDE_DIRECTORIES
- FAM_SCAN_EXCLUDE_EXTENSIONS
- FAM_SCAN_EXCLUDE_FILES
- FAM_SCAN_MAX_DEPTH

Tema principal: Resolución de problemas de la actividad de archivos

Faltan resultados de clasificación de archivos en los informes y el panel de control de investigación

Síntomas

Faltan resultados de clasificación de archivos en los informes y en el panel de control de investigación.

Causas

La clasificación es un proceso adicional que va más allá del descubrimiento de metadatos.

Resolución del problema

Suponiendo que se cumplan los requisitos de software para el motor de IBM Content Classification (http://www-01.ibm.com/support/docview.wss?uid=swg27020838) que se utiliza para la clasificación, verifique las siguientes configuraciones de GIM:

- Asegúrese de que el parámetro de GIM FAM_IS_DEEP_ANALYSIS=TRUE
- Verifique que los nombres del plan de decisiones sean correctos en el valor FAM_ICM_CLASS_DECISION_PLANS y que la lista de planes de decisiones esté delimitada con un punto y coma
- Verifique que existan todos los planes de decisiones (,dpn) listados en la siguiente ubicación del servidor de archivos: %FAM_HOME%\conf\ContentClassification

Respuesta del usuario: Opcional. Cuando tenga acciones concretas que realicen usuarios específicos, utilice uno o varios de los elementos ts*Response.

Tema principal: Resolución de problemas de la actividad de archivos

El paquete de FAM no se puede instalar

Después de instalar el cliente de GIM, la instalación del paquete de FAM falla.

Síntomas

Cuando se intenta instalar el paquete de FAM, el sistema responde con un mensaje parecido a:

```
-1,GIM - Failure point : dependancy_violation (Dependancy violation (FAM) : Missing mandatory dependency - STAP at GIM.pm line
3176, <MYFILE> line 20.
```

Causas

El paquete de S-TAP debe estar instalado antes de instalar el paquete de FAM.

Resolución del problema

Instale el paquete de FAM. Consulte Instalación y activación de componentes de supervisión de actividad de archivos.

Tema principal: Resolución de problemas de la actividad de archivos

Instalación del sistema Guardium

- Error de suma de comprobación durante la instalación de S-TAP
  Si recibe un error de suma de comprobación, establezca la modalidad de transferencia en binario en el cliente FTP.
- S-TAP de Guardium devuelve un mensaje de error de cp: opción -f no permitida
  Si la instalación de S-TAP falla con cp: option -f no permitida, ejecute el mandato que cp y cambie la vía de acceso del archivo.
- La instalación de un nuevo parche de Guardium no se completa
  Si no puede completar la instalación de un nuevo parche de Guardium, detenga el proceso que interfiere y vuelva a instalar el parche.
- Falta un archivo o directorio después de una instalación nueva de S-TAP de Guardium
- Error de partición al instalar Guardium
  Si recibe un error de partición, seleccione la instalación Personalizada y especifique explícitamente el tamaño y la ubicación del disco.
- Falla la instalación de parche: no existe ese archivo o directorio
  Si la instalación de parche falla, compruebe que el archivo coincida con el MD5SUM del parche descargado.

Tema principal: Problemas y soluciones

Error de suma de comprobación durante la instalación de S-TAP

Si recibe un error de suma de comprobación, establezca la modalidad de transferencia en binario en el cliente FTP.

Síntomas

Recibe un error similar al siguiente cuando ejecuta el instalador de S-TAP para instalar S-TAP de Guardium en UNIX o Linux.

```
./guard-stap-v81_r26808_1-aix-6.1-aix-powerpc.sh
Verificando la integridad del archivador...Error in sumas de comprobación: 2082112805 es
distinto de 3728267449
```

Causas

El archivo del instalador está dañado. El archivo se ha dañado al transferir el archivo al servidor de base de datos o al descargar el producto.

Entorno

Afecta a S-TAP en UNIX o Linux.

Resolución del problema

Para resolver el problema, asegúrese de que la modalidad de transferencia esté establecida en binaria en el cliente FTP. A continuación, intente de nuevo la transferencia al servidor de base de datos. Si el proceso falla, descargue el producto de nuevo.

Tema principal: Instalación del sistema Guardium

S-TAP de Guardium devuelve un mensaje de error de cp: opción -f no permitida

Si la instalación de S-TAP falla con cp: option -f no permitida, ejecute el mandato que cp y cambie la vía de acceso del archivo.

Síntomas

La instalación de S-TAP falla con el mensaje de error siguiente.

```
A directory called 'guardium' containing Guardium software needs to be created under a path provided.
Enter the path prefix [/usr/local]? /opt/guardium
Directory /opt/guardium/guardium/guard_stap does not exist, would you like to create it [Y/n]? Y
Run STAP as root, or as user 'guardium' [R/u]? R
Please be patient... This might take more than a minute.
Copying installation files...
cp: illegal option -- f
UX:vxfs cp: INFO: V-3-21462: Usage: cp [-i] [-p] f1 f2
cp [-i] [-p] f1 ... fn d1
cp [-i] [-p] [-r|-R] [-e { force | ignore | warn}] d1 d2
```

Causas

La vía de acceso de /usr/bin/cp es distinta de lo que espera el instalador.

Entorno

Afecta al servidor de base de datos UNIX/Linux.

Resolución del problema

Ejecute el mandato which cp

Si which cp devuelve un valor distinto de /usr/bin/cp, ejecute el mandato export PATH=/usr/sbin:/usr/bin:$PATH.

Vuelva a ejecutar el mandato which cp para confirmar que la vía de acceso es /usr/bin/cp.

Tema principal: Instalación del sistema Guardium

La instalación de un nuevo parche de Guardium no se completa

Si no puede completar la instalación de un nuevo parche de Guardium, detenga el proceso que interfiere y vuelva a instalar el parche.

Síntomas

Cuando se instala un parche nuevo, éste no se completa. La columna de estado en el mandato de CLI show system patch installed muestra uno de los mensajes siguientes.

```
STEP: Setting “java” off
STEP: Setting “amei” off
STEP: Setting “sqlw” off
```

Causas

Tomcat, el núcleo de inspección, u otro proceso de la máquina ha interferido con la instalación del parche.

Entorno

Afecta al recopilador, al agregador y al gestor central.

Resolución del problema

Para instalar el nuevo parche de Guardium, detenga los procesos que interfieren con la instalación.

1. Suprima el parche que está atascado mediante el mandato delete scheduled-patch.
2. Reinicie el sistema mediante el mandato restart system.
3. Cuando se reinicie el sistema, detenga la interfaz gráfica de usuario y los núcleos de inspección mediante los mandatos stop gui y stop inspection-core.
4. Reinstale el parche y reinicie la interfaz gráfica de usuario y el núcleo de inspección mediante los mandatos restart gui y start inspection-core.

Tema principal: Instalación del sistema Guardium

Falta un archivo o directorio después de una instalación nueva de S-TAP de Guardium

Síntomas

Cuando intenta instalar S-TAP, recibe el mensaje de error siguiente.

```
Tap_controller::init failed Opening pseudo device /dev/guard_ktap No such file or directory
```

Además, /dev/*ktap* no existe.

Causas

Hay muchas razones posibles por las que la creación del dispositivo K-TAP puede fallar. A continuación se muestran las causas más comunes.

- No ha utilizado los archivos de módulo, incluido el módulo K-TAP para el kernel de Linux.
- No ha especificado la opción Flex Loading para cargar el módulo K-TAP a partir de los archivos de módulo.
- Un módulo K-TAP anterior de una instalación anterior sigue en ejecución o instalado.

Entorno

Afecta a todos los sistemas operativos Linux y UNIX en los que se puede instalar el producto S-TAP de IBM Guardium.

Resolución del problema

Para resolver el problema, realice los pasos siguientes.

1. Ejecute estos mandatos como root.

   ```
   <directorio de STAP>/KTAP/guard_ktap_loader stop
   <directorio de STAP>/KTAP/guard_ktap_loader uninstall
   <directorio de STAP>/KTAP/guard_ktap_loader install
   <directorio de STAP>/KTAP/guard_ktap_loader start
   ```

2. Compruebe si el dispositivo K-TAP se ha creado ahora con el mandato ls /dev/*ktap *. Si se ha creado, el problema está resuelto. Si no es así, continúe con el paso siguiente.
3. Detenga el proceso de S-TAP guard_stap, si se está ejecutando. Puede comprobar si se está ejecutando con el mandato ps -ef | grep guard_stap.
4. Verifique que el proceso de S-TAP no se esté ejecutando con el mandato ps -ef | grep guard_stap.
5. Desinstale el S-TAP.
6. Confirme que el directorio de S-TAP ha desaparecido.
7. Compruebe si aún se está ejecutando un módulo de K-TAP de una instalación anterior. Utilice el mandato apropiado para el sistema operativo.

   ```
   Linux    : lsmod | grep ktap
   Solaris  : modinfo | grep  tap
   HP-UX    : lsdev | grep tap
   AIX      : genkex | grep tap
   ```

   Si un dispositivo como ktap_<release> aparece en la lista, hay un módulo K-TAP en ejecución.
8. Si encuentra en el paso anterior que un módulo K-TAP se está ejecutando, ejecute los pasos siguientes para detener y desinstalar el módulo K-TAP.

   ```
   <directorio de STAP>/KTAP/guard_ktap_loader stop
   <directorio de STAP>/KTAP/guard_ktap_loader uninstall
   ```

   Reinicie el servidor.
9. Si está utilizando Guardium Installation Manager (GIM), vaya a Gestionar > Instalación de módulo > Configuración por cliente (Antiguo), seleccione el cliente y, a continuación, pulse Restablecer clientes. Espere a que el servidor aparezca de nuevo en la lista de clientes de la interfaz gráfica de usuario de GIM (normalmente unos minutos).
10. Vuelva a instalar el S-TAP. Si utiliza GIM para instalar el S-TAP, vuelva a instalar el paquete S-TAP con GIM y los mandatos siguientes.

    ```
    KTAP-ALLOW_COMBOS=Y
    KTAP_LIVE_UPDATE=Y
    KTAP_ENABLED=Y
    ```

Tema principal: Instalación del sistema Guardium

Error de partición al instalar Guardium

Si recibe un error de partición, seleccione la instalación Personalizada y especifique explícitamente el tamaño y la ubicación del disco.

Síntomas

Cuando se instala el dispositivo de Guardium en VMWare, se recibe el error siguiente:

```
Error al particionar
No se ha podido asignar las particiones solicitadas:
El particionamiento ha fallado: No se han podido asignar particiones como particiones primarias.
No queda espacio suficiente para crear partición para /boot.
```

Causas

Cuando se instala el sistema Guardium con VMWare, si selecciona Típico, VMWare utiliza los parámetros de configuración predefinidos para el tipo de SO en VMWare. Es posible que estos parámetros de configuración no sean adecuados para esta instalación.

Entorno

Afecta a todas las configuraciones de Guardium (recopilador, agregador, gestor central).

Resolución del problema

Seleccione la instalación Personalizada y especifique explícitamente el tamaño y la ubicación del disco. Especifique un tamaño de disco que sea suficientemente grande para sus necesidades de supervisión y auditoría. Una vez configurado, Guardium no da soporte a la adición de espacio de disco al sistema.

Tema principal: Instalación del sistema Guardium

Falla la instalación de parche: no existe ese archivo o directorio

Si la instalación de parche falla, compruebe que el archivo coincida con el MD5SUM del parche descargado.

Síntomas

La instalación de parches en Guardium falla con el error `patch.reg: No such file or directory`.

Causas

Los casos siguientes pueden causar que la instalación de parche falle.

- El parche no se ha descargado en modalidad binaria y el archivo se ha dañado.
- El archivo comprimido en sí se ha subido al sistema Guardium.
- El parche se ha recibido del soporte de Guardium y tiene como prefijo del nombre de archivo el número de PMR.
- El parche se ha subido al sistema Guardium desde un servidor FTP de Windows.

Entorno

Afecta al recopilador, al agregador y al gestor central.

Resolución del problema

Verifique que el contenido del archivo coincida con el MD5SUM del parche descargado. Si el archivo comprimido no se puede extraer o si el MD5SUM no coincide, descargue el archivo en modalidad binaria.

Si el propio archivo comprimido se ha subido al sistema Guardium, extraiga el archivo comprimido y suba sólo el parche.

Si el nombre de archivo tiene como prefijo un número de PMR, elimine el número y, a continuación, suba el parche al sistema Guardium.

Si el parche se ha subido desde un servidor FTP de Windows, especifique el nombre de archivo exacto con las mayúsculas y minúsculas correctas.

Tema principal: Instalación del sistema Guardium

S-TAPs y otros agentes

Guardium S-TAPs es un agente de software ligero que se instala en un servidor de base de datos o en un sistema servidor de archivos. El S-TAPs supervisa el tráfico de archivos o de bases de datos y reenvía información acerca de dicho tráfico a un sistema Guardium. Otros agentes, incluidos K-TAPs y A-TAPs, realizan funciones complementarias.

- Instalación de S-TAP
  Puede instalar S-TAP en servidores con bases de datos o sistemas de archivos que desee supervisar. Hay varias opciones para instalar un S-TAP.
- Equilibrio de carga empresarial
  El equilibrador de carga empresarial asigna de forma dinámica unidades gestionadas a agentes de S-TAP en función de la carga y la disponibilidad del sistema.
- Tráfico de base de datos autenticado mediante Kerberos
- Utilización de bibliotecas de salida
  Las bibliotecas de salida incluyen una biblioteca de Guardium en la base de datos, utilizando el mecanismo de salida. La biblioteca, o módulo, de salida permite la comunicación directa entre el S-TAP de Guardium para reenviar el tráfico de la base de datos.
- Configuración especial de entornos Linux, Solaris, HP-UX y AIX
  Utilice estos procedimientos para los correspondientes sistemas con zonas, RAC, particiones de carga de trabajo (WPAR) o clústeres.
- Guía de administración de S-TAP
  Guardium S-TAP es un agente de software ligero instalado en un sistema servidor de base de datos.
- Configuración del sistema Guardium para gestionar S-TAP
  Para poder gestionar un S-TAP desde la GUI de Guardium, configure el sistema Guardium y reinicie los motores de inspección.

- Certificación de S-TAP
  Utilice esta función para evitar que los S-TAP no autorizados se conecten al sistema Guardium.
- Configuración de la autenticación de S-TAP con certificados SSL
  Configure la autenticación entre un servidor S-TAP y el sistema Guardium.
- Aumento del rendimiento de S-TAP
  Puede configurar un S-TAP que notifique a varios sistemas Guardium para aumentar el rendimiento de los datos.
- S-TAP de UNIX
  Instalación y configuración de S-TAP de UNIX.
- S-TAP de Windows
  Utilice esta sección para ver información de configuración de S-TAP de Windows.
- S-TAP Discovery
  Habilite S-TAP para descubrir de forma periódica instancias de bases de datos y enviar los resultados al sistema S-TAP activo actual.
- Gestión de A-TAP
  A-TAP es una abreviación de TAP a nivel de aplicación (Application-level TAP). Un A-TAP se ubica en la capa de la aplicación para dar soporte a la supervisión del tráfico de base de datos cifrado, lo que no es posible realizar en el kernel mediante un K-TAP.
- Tee
  Tee ha quedado en desuso y se encuentra aquí sólo como referencia.
- Configuración de S-TAP desde la GUI
  Después de instalar un agente de S-TAP en un servidor de base de datos, la configuración de S-TAP se puede realizar desde la GUI.
- Edición de los parámetros de configuración de S-TAP
  Hay varias formas de modificar la configuración de un S-TAP después de instalarlo.
- Configuración del montaje retardado en disco de clúster
  Este tema sólo se aplica a los servidores de base de datos Oracle, Informix y DB2.
- Supervisor de estado de S-TAP
  El supervisor de estado de S-TAP le permite ver el estado actual de los S-TAP e investigar los problemas.
- Visualización de los resultados de la verificación de S-TAP
  El proceso de verificación de S-TAP comprueba varios parámetros de configuración e intenta conectarse a los motores de inspección. Puede ver los resultados en la página Supervisor de estado de S-TAP.
- Configuración de la planificación de verificación de S-TAP
  Puede configurar la planificación para ejecutar la verificación de S-TAP.
- Resolución de problemas de S-TAP en la plataforma Linux
  Puede utilizar el separador del supervisor de estado de S-TAP de la vista del sistema para empezar a investigar cualquier problema. A veces, es posible que tenga que utilizar otras herramientas, especialmente si está supervisando bases de datos para las que no se pueden verificar los motores de inspección.
- Supervisión del comportamiento de S-TAP
  S-TAP Monitor (guard_monitor) es un proceso diseñado para supervisar el rendimiento y la capacidad de respuesta de S-TAP. Se pueden llevar a cabo determinadas acciones en función de diversos umbrales.
- Panel de sucesos de S-TAP
  Puede utilizar el panel Sucesos S-TAP para ver la salida de los mensajes de sucesos generados por S-TAP.
- Informes de S-TAP
  De forma predeterminada, los informes que se describen en este tema aparecen en el panel Informes.
- Mensajes de error de S-TAP
  En la lista siguiente se describen los mensajes de error que genera S-TAP, en orden alfabético.
- Apéndice de S-TAP
  En esta sección se explica cómo pasar de una versión de Informix a otra.
- Instalación, inicio y detención de CAS desde la línea de mandatos
  Utilice los siguientes mandatos para instalar, iniciar y detener CAS.
- Definiciones de IMS
  Una definición de IMS establece una conexión entre el sistema Guardium y el entorno de IMS que desea auditar.
- DB2 for i S-TAP
  Puede utilizar el S-TAP Guardium DB2 for i para supervisar e informar sobre cualquier acceso a base de datos en IBM i. Esto incluye cualquier programa, como por ejemplo RPG, que utilice operaciones de E/S nativas de base de datos o acceso SQL.
- IBM Security Guardium S-TAP for z/OS
  La solución IBM Security Guardium S-TAP for z/OS es una herramienta que recopila y correlaciona información de acceso a datos para DB2 en z/OS, Data Sets en z/OS o IMS en z/OS para generar una vista completa de la actividad empresarial para los auditores.

Instalación de S-TAP

Puede instalar S-TAP en servidores con bases de datos o sistemas de archivos que desee supervisar. Hay varias opciones para instalar un S-TAP.

Visión general de la instalación de S-TAP

Cuando se instala S-TAP en un servidor de base de datos, se debe especificar la dirección IP o el nombre de host completo del sistema Guardium que recibirá los datos de S-TAP. Después de que el S-TAP se haya conectado al sistema Guardium, todos los parámetros de configuración del S-TAP restantes se pueden especificar desde la consola de administración en el sistema Guardium.

Nota: Durante la instalación, el instalador de S-TAP comprueba si K-TAP está disponible para la versión del kernel. Si el K-TAP no se puede instalar o no se inicia, se consulta al usuario si se debe continuar con la instalación.

El directorio de instalación para el S-TAP debe estar vacío o no existir. No puede instalar un S-TAP en un directorio que ya contenga archivos.

Antes de instalar un S-TAP, consulte los requisitos del sistema para IBM Security Guardium versión 10.1 para asegurarse de que se da soporte a las versiones de la base de datos y del sistema operativo.

Hay dos tareas principales que debe realizar para instalar y empezar a utilizar un S-TAP:

1. Instalar el S-TAP en un servidor de base de datos.
2. Configurar el S-TAP de modo que supervise el tráfico adecuado.

Estas tareas se explican en esta sección y en las siguientes.

Métodos de instalación

El método recomendado para instalar S-TAP y otros agentes en los servidores de base de datos es mediante Guardium Installation Manager (GIM). GIM le permite instalar, actualizar y gestionar agentes en servidores individuales o grupos de servidores. GIM también supervisa los procesos que se han instalado bajo su control. Puede utilizar GIM para modificar parámetros y realizar otras tareas de gestión. Consulte la sección sobre Guardium Installation Manager para ver detalles sobre GIM.

En algunos casos, es posible que prefiera instalar el S-TAP localmente. Puede hacerlo utilizando un instalador interactivo o la línea de mandatos. Estos métodos se describen en esta sección.

Cuando se instala un S-TAP en un servidor UNIX, el programa de instalación comprueba si existe el grupo de guardium. Si el grupo no existe, el programa de instalación lo crea. Si utiliza determinados componentes o características, como por ejemplo A-TAP o DB2 Exit, debe añadir usuarios a este grupo para garantizar su correcto funcionamiento. Estos requisitos se describen en las secciones relevantes de esta información.

Requisitos previos de la instalación de S-TAP

En las tablas siguientes se muestran los componentes de base de datos que se deben instalar, a un determinado nivel de release o de parche, o configurados para dar soporte a S-TAP.

Tabla 1. Componentes de base de datos

Componente	Requisito previo
CAS bajo HP-UX	Java™ 1.5 o superior
CAS bajo cualquier otro UNIX	Java 1.4.2 o superior
CAS bajo Windows	Si CAS va a supervisar el registro de sucesos de MS SQL Server, se debe instalar el programa dumpel.exe desde el Kit de recursos de Microsoft Windows en el servidor de base de datos. Compruebe si existe este programa en el directorio c:\Files\Resource Kit\. Si no es así, puede descargarlo desde Microsoft.
S-TAP, todo UNIX	Si se utilizan el método de supervisión Tee y el componente Hunter, Perl 5.8.0 o posterior
S-TAP en Red Hat Linux V4	Make versión 3.81 o posterior. Para ver su versión del programa de utilidad make, emita este mandato: `make -v`
Oracle ASO, SSL AIX - todo	Para AIX 5.3, se necesita el nivel de tecnología 5 o posterior para dar soporte a LDR_PRELOAD. Los sistemas AIX 6 y 7 incluyen este soporte.
Oracle ASO, HP-UX 11.11	LD_PRELOAD debe estar instalado. Se instala con el parche PHSS_28436 o posterior.
TLS	Para S-TAP en un servidor UNIX, debe aparecer /dev/random o /dev/urandom en el servidor. Tanto para servidores UNIX como para servidores Windows, consulte los requisitos de puerto de Guardium y compruebe los requisitos de puerto de TLS

Nota: Durante una instalación o actualización, es posible que JVM genere un error para Java 1.6.0 que indica que no encuentra la DLL. No se ha encontrado la biblioteca de enlaces dinámicos MSVCR71.dll en la vía de acceso especificada. Este error se puede solucionar implementando uno de los dos métodos alternativos: 1) utilizar una JVM diferente (otra versión) (si hay una disponible en el sistema) o 2) descargar la DLL de Microsoft y colocarla en el directorio del sistema Windows.
Nota:

Si instala GIM o S-TAP, deberá ser un usuario root para crear y suprimir usuarios y grupos.

Tabla 2. Tipo de requisito por plataforma

Tipo de requisito	HP-UX	Solaris	AIX	Linux
el archivo existe	/bin/sh	/bin/sh	/bin/sh	/bin/sh
el archivo existe	/bin/sed o /usr/bin/sed	/bin/sed o /usr/bin/sed	/bin/sed o /usr/bin/sed	/bin/sed o /usr/bin/sed
el archivo existe	tar, awk, grep, tr	tar, awk, grep, tr	tar, awk, grep, tr	tar, awk, grep, tr
el archivo existe	prealloc	dd y /dev/zero	dd y /dev/zero	dd y /dev/zero
el archivo existe	uudecode en /usr/bin o /tmp o perl existe	uudecode en /usr/bin o /tmp o perl existe	uudecode en /usr/bin o /tmp o perl existe	uudecode en /usr/bin o /tmp o perl existe

S-TAP y CAS - Requisitos de espacio de disco

Tabla 3. Requisitos de espacio de disco

Espacio de disco	Descripción
Archivos de programa de S-TAP	AIX: 300 MB HP-UX: 400 MB Linux: 350 MB Solaris: 300 MB Windows: 180 MB para instalación no GIM AIX: 400 MB HP-UX: 500 MB Linux: 450 MB Solaris: 400 MB Windows: 300 MB para instalación GIM Archivos de programa de FAM para UNIX - 600 MB como mínimo
Archivos de programa de CAS incluido Java	AIX: 309 MB HP-UX: 630 MB Linux: 405 MB Solaris: 390 MB Windows: 277 MB

Espacio de disco	Descripción
Archivo de almacenamiento intermedio	De forma predeterminada, S-TAP utiliza memoria anónima para transferir datos al sistema Guardium. Si configura el S-TAP de modo que utilice un archivo de almacenamiento intermedio, el tamaño predeterminado es 100 MB. El tamaño se controla mediante el parámetro del archivo de configuración buffer_file_size.
Java	Si se utiliza CAS, se necesita Java. En un servidor UNIX, debe obtener e instalar Java usted mismo (debido a restricciones de licencia). Para instalar Java necesitará una determinada cantidad de espacio de disco.
Perl	Solo UNIX. Si se utiliza el mecanismo de recopilación de datos Tee y su componente Hunter opcional, se necesita Perl 5.8.0. Si no se ha instalado anteriormente, deberá obtenerlo e instalarlo usted mismo. Para ver los requisitos de espacio o para descargar Perl, consulte perl.org.

El proceso de instalación para cada componente crea un archivo de registro. Las ubicaciones incluyen /var/tmp y el directorio de instalación del componente.

El proceso de instalación actualiza los scripts inittab, upstart y rc.

Requisitos de puerto de Guardium

Si hay un cortafuegos entre los componentes de Guardium (por ejemplo, entre un sistema Guardium y un S-TAP o un agente CAS en un servidor de base de datos), debe verificar que los puertos utilizados para las conexiones entre esos componentes no se están bloqueadas. Consulte la Tabla 4 y utilice el programa de utilidad de gestión de cortafuegos para comprobar (y posiblemente abrir) los puertos adecuados.

Tabla 4. Requisitos de puerto para servidores UNIX

Puerto	Protocolo	Conexión del sistema Guardium con ...
16016	TCP	UNIX S-TAP despejado (abra el puerto)
16017	TCP	UNIX CAS desplegado (abra el puerto)
16018	TLS	UNIX S-TAP cifrado
16019	TLS	UNIX CAS cifrado
16020-16021		Utilizado para conexiones agrupadas
16022		Protocolo de canal de información

Tabla 5. Requisitos de puerto para servidores Windows

Puerto	Protocolo	Conexión del sistema Guardium con ...
8075	UDP	Señal de latido de Windows S-TAP Nota: El agente Unix S-TAP no utiliza UDP para señales de latido, por lo que no hay ningún puerto Unix correspondiente para esta función.
9500	TCP	Windows S-TAP desplegado (abra el puerto)
9501	TLS	Windows S-TAP cifrado
16017	TCP	Windows CAS desplegado (abra el puerto)
16019	TLS	Windows CAS cifrado

Cuando instale un agente S-TAP o CAS en un servidor de base de datos, resulta muy útil verificar que hay conectividad entre este servidor y el sistema Guardium. En un sistema UNIX, puede utilizar el mandato nmap para comprobar la conectividad, utilizando las siguientes opciones:

```
nmap -p <port> <ip_address>
```

Por ejemplo, para comprobar que se puede acceder al puerto 16018 (el puerto de Guardium utilizado para TLS) en la dirección IP 192.168.3.104, especifique este mandato:

```
nmap -p 16018  192.168.3.104 Starting nmap V. 3.00 Interesting ports on g4.guardium.com (192.168.3.104): Port       State
Service 16018/tcp  open        unknown
```

- Instalación de un S-TAP en un servidor Windows
  Instale un S-TAP en Windows utilizando Guardium Installation Manager (GIM), el instalador interactivo o el instalador de línea de mandatos.
- Instale el cliente de S-TAP en un servidor Linux, Solaris, AIX o HP-UX
  Puede instalar el cliente de S-TAP en un servidor Linux, Solaris, AIX o HP-UX con: Guardium Installation Manager (GIM), el RPM, el instalador del shell o el instalador nativo. Utilice el método que mejor se adapte a sus necesidades.
- Cuándo reiniciar o rearrancar la base de datos después de la instalación o actualización de S-TAP
  En este tema se detallen los casos, después de la instalación de S-TAP, en que se debe reiniciar o se debe rearrancar la instancia de la base de datos o el servidor de base de datos. Se cubren los S-TAP tanto de Windows como de UNIX/Linux. Se cubren las versiones v9.0/9.1/9.5 y v10.0/10.1. Los requisitos de reinicio/rearranque son los mismos para las implementaciones de GIM y no de GIM.

Tema principal: S-TAPs y otros agentes

Instalación de un S-TAP en un servidor Windows

Instale un S-TAP en Windows utilizando Guardium Installation Manager (GIM), el instalador interactivo o el instalador de línea de mandatos.

En función de la clave de licencia, puede utilizar el mismo agente de S-TAP para la supervisión de actividades de base de datos y de archivos. No hay parámetros específicos para FAM.

Dispone de cuatro métodos para instalar un S-TAP en un sistema Windows:

Herramienta para desplegar agentes de supervisión
: A partir de Guardium V. 10.1.3, puede activar automáticamente clientes GIM, instalar S-TAP y empezar a supervisar el tráfico de base de datos. Consulte Inicio rápido para desplegar agentes de supervisión

Guardium Installation Manager

GIM es el método recomendado para instalar S-TAPs en los servidores. GIM le permite instalar, actualizar y gestionar agentes en servidores individuales o grupos de servidores. Esto incluye la supervisión de los procesos que se han instalado bajo su control, la modificación de los parámetros del agente y la realización de otras tareas de gestión. Para obtener más información, consulte Instalación de S-TAP de Windows mediante Guardium Installation Manager.

Instalador interactivo

El instalador interactivo resulta útil para despliegues pequeños o siempre que se necesite una experiencia guiada de instalación paso a paso. Proporciona un sistema de validación en cada paso, lo que significa menos probabilidades de errores. Para obtener más información, consulte Instalación de S-TAP de Windows mediante el instalador interactivo.

Nota: Los parámetros de S-TAP de Windows no se pueden cambiar mediante el instalador interactivo durante una actualización. El usuario puede utilizar la GUI después de la actualización para cambiar los parámetros de S-TAP de Windows.

Instalador de línea de mandatos

El instalador de línea de mandatos para S-TAP en Windows proporciona una solución de script que resulta especialmente útil para gestionar despliegues grandes. Para obtener más información, consulte Instalación de Windows S-TAP mediante la interfaz de línea de mandatos.

Nota: La instalación de S-TAP de Windows requiere una carpeta nueva o vacía para la instalación.
Nota: El servicio Base Filtering Engine (BFE) se debe estar ejecutando para la instalación de S-TAP. Si el servicio existe pero no está en ejecución, Guardium intentará iniciarlo.
Nota: Los S-TAP V10.0 y V10.1 necesitan .NET Framework versión 4.5 o posterior. Si el entorno .NET 4.5 o posterior no existe, S-TAP instalará .NET 4.5.2.
Nota:

Al instalar el S-TAP de Windows en un entorno no ASCII (por ejemplo, en un entorno japonés), el usuario tiene que utilizar el servidor con ese paquete de idiomas o establecer el entorno local del sistema para esa ubicación (Japón).

Descubrimiento automático de bases de datos

Cuando instala un S-TAP en Windows, tiene la opción de descubrir automáticamente bases de datos y de crear motores de inspección para las bases de datos descubiertas. El proceso de descubrimiento automático se ejecuta una vez en el momento de la instalación de S-TAP y no se repite automáticamente.

Durante una actualización, el descubrimiento automático crea motores de inspección para cualquier base de datos recién descubierta y ajusta los motores de inspección ya existentes. Esto significa que, si ha añadido un motor de inspección para una base de datos que no existe o ha especificado un puerto que no funciona, el proceso de descubrimiento automático ajustará ese motor de inspección durante la actualización.

Si no desea que la instalación de S-TAP realice el descubrimiento automático de bases de datos durante la instalación o actualización, puede evitarlo durante el proceso de instalación de S-TAP siguiendo el procedimiento descrito para cada instalador de S-TAP de Windows.

Equilibrio de carga empresarial

Durante la instalación de un S-TAP en Windows, puede configurar el S-TAP de modo que utilice las características de equilibrio de carga. Para obtener más información, consulte Equilibrio de carga empresarial.

- Instalación de S-TAP de Windows mediante Guardium Installation Manager
  Guardium Installation Manager (GIM) es el método recomendado para instalar S-TAPs en los servidores de base de datos.
- Instalación de S-TAP de Windows mediante el instalador interactivo
  El instalador interactivo resulta útil para despliegues pequeños o siempre que se necesite una experiencia guiada de instalación paso a paso.
- Instalación de Windows S-TAP mediante la interfaz de línea de mandatos
  El instalador de línea de mandatos proporciona una solución de script que resulta especialmente útil para gestionar despliegues de gran tamaño.
- Referencia de la instalación desde la línea de mandatos de S-TAP de Windows
  El instalador de línea de mandatos le permite crear scripts que resultan especialmente útiles para gestionar despliegues de gran tamaño. Esta referencia contiene los parámetros (cada uno con una breve descripción) que se pueden utilizar con en los scripts.
- Actualización y eliminación de un S-TAP en Windows
  Aprenda a actualizar o a eliminar un S-TAP en Windows.

Tema principal: Instalación de S-TAP
Conceptos relacionados:
Instalación de S-TAP
Guardium Installation Manager
Equilibrio de carga empresarial

Instalación de S-TAP de Windows mediante Guardium Installation Manager

Guardium Installation Manager (GIM) es el método recomendado para instalar S-TAPs en los servidores de base de datos.

Antes de empezar

Verifique lo siguiente antes de empezar:

- Revise los requisitos de instalación de S-TAP de Windows en Instalación de S-TAP.
  - Verifique que el servidor de base de datos y el sistema operativo reciben soporte.
  - Identifique los puertos necesarios para la comunicación entre el S-TAP y el sistema Guardium.
- Abra los puertos de cortafuegos utilizados para la comunicación entre el S-TAP y el sistema Guardium.
- Verifique que el directorio en el que va a instalar el S-TAP esté vacío o que no exista.
- El cliente GIM está instalado en el servidor de base de datos en el que instalará un S-TAP.
- El cliente GIM del servidor de base de datos se comunica con el sistema Guardium.

Acerca de esta tarea

Después de instalar un cliente GIM en el servidor de base de datos, la instalación de módulos como S-TAP para Windows se planifica desde el sistema Guardium.

Procedimiento

1. Suba el módulo de S-TAP de Windowspara instalarlo.
   a. En el sistema Guardium, vaya a Gestionar > Instalación de módulo > Subir módulos.
   b. Pulse Elegir archivo y seleccione el módulo de S-TAP que desea instalar.
   c. Pulse Subir para subir el módulo al sistema Guardium. Después de subirlo, el módulo aparecerá en la lista de la tabla Importar módulos subidos.
   d. En la tabla Importar módulos subidos, marque el recuadro de selección situado junto al módulo de S-TAP que desea instalar. El módulo se importará y estará listo para su instalación. Después de importar el módulo, se restablecerá la página Subir módulos y la tabla Importar módulos subidos estará vacía.
2. Seleccione los sistemas cliente en los que desea instalar un S-TAP.
   a. Navegue a Gestionar > Instalación de módulo > Configuración por cliente (Antiguo).
   b. En la pantalla Criterios de búsqueda de cliente, especifique criterios de búsqueda para los clientes donde desea instalar el S-TAP y, a continuación, pulse Buscar para continuar. Puede buscar clientes utilizando cualquier combinación de los siguientes criterios de búsqueda:
      - Seleccionar un grupo de clientes.
      - Buscar por nombre de host, dirección IP o sistema operativo.
      - Deje todos los campos de criterios de búsqueda vacíos para volver una lista de todos los clientes disponibles.
   c. En la pantalla Clientes, marque el recuadro de selección situado junto a los clientes donde desea instalar el S-TAP y, a continuación, pulse Siguiente para continuar.
3. Seleccione y configure el módulo de S-TAP antes de instalarlo en los sistemas cliente.
   a. En la tabla Módulos de la pantalla Módulos comunes, seleccione el módulo de S-TAP que desea instalar y pulse Siguiente para continuar.
      - Utilice los recuadros de selección Visualizar las últimas versiones y Visualizar solo lotes para filtrar la lista de módulos disponibles.
      - Utilice la tabla Estado de módulo para revisar la información sobre el módulo seleccionado en los clientes de destino.
   b. En la pantalla Parámetros de módulo de cliente, especifique los parámetros de instalación para el S-TAP.
      - Para aplicar los mismos parámetros a varios clientes, especifique parámetros de instalación en los campos Parámetros de módulo comunes, marque el recuadro de selección que hay junto a los clientes que aparecen en las tablas Parámetros de módulo de cliente y pulse Aplicar a seleccionados.
      - Para aplicar parámetros exclusivos a clientes individuales, especifique los parámetros de instalación directamente en la tabla Parámetros de módulo de cliente.

      Atención:
      - Aunque los parámetros predeterminados resultan aceptables para la mayoría de las instalaciones, se le solicitará que proporcione un valor para WINSTAP_INSTALL_DIR. El valor predeterminado es C:/Program Files/IBM/Windows S-TAP.
      - Si no se especifica WINSTAP_TAP_IP (equivalente al parámetro de línea de mandatos -taphost), se utiliza el valor GIM_CLIENT_IP.
      - Si no se especifica WINSTAP_SQLGUARD_IP (equivalente al parámetro de línea de mandatos -appliance), se utiliza el valor GIM_URL.
   c. Cuando haya especificado los parámetros de instalación para el S-TAP, aplique dichos parámetros a los clientes seleccionados pulsando Aplicar a cliente.
4. Por último, instale el S-TAP en los clientes seleccionados.
   a. Desde la pantalla Parámetros de módulo de cliente, pulse Instalar/Actualizar.
   b. En el diálogo Fecha de planificación, especifique una fecha u hora para iniciar la instalación y pulse Aplicar. Para empezar la instalación inmediatamente, utilice el valor `ahora` en el campo Fecha de planificación.

Qué hacer a continuación

Supervise la instalación del módulo de S-TAP utilizando la tabla Estado de módulo de la pantalla Módulos comunes. También puede ver el estado de la instalación del módulo consultando el informe en Gestionar > Informes > Gestión de instalación > Estado de clientes de GIM.

Verifique que el S-TAP se está comunicando con el sistema Guardium; para ello, vaya a Gestionar > Supervisión de actividad > Control de S-TAP y revise el estado y la configuración de S-TAPs.

Tema principal: Instalación de un S-TAP en un servidor Windows
Conceptos relacionados:
Guardium Installation Manager

Instalación de S-TAP de Windows mediante el instalador interactivo

El instalador interactivo resulta útil para despliegues pequeños o siempre que se necesite una experiencia guiada de instalación paso a paso.

Antes de empezar

Verifique lo siguiente antes de empezar:

- Revise los requisitos de instalación de S-TAP de Windows en Instalación de S-TAP.
  - Verifique que el servidor de base de datos y el sistema operativo reciben soporte.
  - Identifique los puertos necesarios para la comunicación entre el S-TAP y el sistema Guardium.
- Abra los puertos de cortafuegos utilizados para la comunicación entre el S-TAP y el sistema Guardium.
- Identifique la dirección IP del servidor de base de datos o del controlador de dominio donde instalará el S-TAP, incluidas las direcciones IP virtuales.
- Identifique la dirección IP del sistema Guardium que controlará el S-TAP.
- Verifique que el directorio en el que va a instalar el S-TAP esté vacío o que no exista.

Acerca de esta tarea

Cuando se instala un S-TAP en un servidor de base de datos, se debe proporcionar la dirección IP o el nombre de host del sistema Guardium que recibirá los datos de S-TAP. Después de que el S-TAP se haya conectado al sistema Guardium, vaya a la página Gestionar > Supervisión de actividad > S-TAP Control y complete la instalación del S-TAP.

Procedimiento

1. Inicie una sesión en el servidor de base de datos mediante una cuenta de administrador del sistema.
2. Localice e inicie el asistente de instalación S-TAP de Guardium Windows.
   Atención: Cuando instale un S-TAP en Windows 2012 o posterior, debe utilizar privilegios administrativos. Para hacerlo, pulse con el botón derecho del ratón en el instalador y seleccione Ejecutar como administrador.
3. Lea el acuerdo de licencia en la pantalla Licencia de Guardium. Para continuar con la instalación, seleccione Acepto los términos del acuerdo de licencia y pulse Siguiente.

4. Especifique el contenido solicitado en la pantalla Información del cliente y pulse Siguiente para continuar. Los valores predeterminados resultan adecuados para la mayoría de las instalaciones.
5. Seleccione uno de los tipos de instalación siguientes y, a continuación, pulse Siguiente para continuar:
   - Típica: una instalación típica resultará adecuada para la mayoría de los usuarios.
   - Compacta: en una instalación compacta se supone que no son necesarias características adicionales como, por ejemplo, equilibrio de carga empresarial.
   - Personalizada: una instalación personalizada le permite modificar opciones adicionales de instalación de S-TAP como, por ejemplo, opciones de software, directorio de instalación y cuenta del usuario que ejecuta el proceso del S-TAP de Windows.
6. Si lo desea, habilite el equilibrio de carga empresarial marcando el recuadro de selección Habilitar el equilibrio de carga en la pantalla Opciones de equilibrio de carga. Pulse Siguiente para continuar.
   a. Si habilita el equilibrio de carga empresarial, especifique la dirección IP del equilibrador de carga en el campo Dirección de host del equilibrador de carga.
   b. Pulse el botón Opciones avanzadas para especificar todas las opciones adicionales de equilibrio de carga empresarial. Para obtener más información, consulte Equilibrio de carga empresarial.
7. Verifique la Dirección de host de tap de software y especifique Dirección(es) de dispositivo en la pantalla Direcciones de red; a continuación, pulse Siguiente para continuar.
   - La dirección de host de tap de software especifica la dirección de la máquina local donde se está instalando el S-TAP.
   - La dirección o direcciones de dispositivo especifican las direcciones del sistema Guardium que controlarán el S-TAP. Especifique varias direcciones (generalmente no más de tres) en líneas separadas para establecer sistemas de sustitución por anomalía para el S-TAP o cuando configure el equilibrio de carga de S-TAP con el parámetro participate_in_load_balancing.

   Atención: Si no desea que el servicio S-TAP se habilite después de la instalación, elimine la marca del recuadro de selección Iniciar servicio S-Tap. Si se elimina la marca del recuadro de selección Iniciar servicio S-Tap también se inhabilita el descubrimiento automático de bases de datos y la creación de motores de inspección.
8. Después de una instalación correcta se muestra la pantalla Asistente de instalación completado. Pulse Finalizar para cerrar el instalador.

Qué hacer a continuación

Verifique que el S-TAP se está comunicando con el sistema Guardium; para ello, vaya a Gestionar > Supervisión de actividad > Control de S-TAP y revise el estado y la configuración de S-TAPs.

Tema principal: Instalación de un S-TAP en un servidor Windows
Conceptos relacionados:
Equilibrio de carga empresarial

Instalación de Windows S-TAP mediante la interfaz de línea de mandatos

El instalador de línea de mandatos proporciona una solución de script que resulta especialmente útil para gestionar despliegues de gran tamaño.

Antes de empezar

Verifique lo siguiente antes de empezar:

- Revise los requisitos de instalación de S-TAP de Windows en Instalación de S-TAP.
  - Verifique que el servidor de base de datos y el sistema operativo reciben soporte.
  - Identifique los puertos necesarios para la comunicación entre el S-TAP y el sistema Guardium.
- Abra los puertos de cortafuegos utilizados para la comunicación entre el S-TAP y el sistema Guardium.
- Identifique la dirección IP del servidor de base de datos o del controlador de dominio donde instalará el S-TAP, incluidas las direcciones IP virtuales.
- Identifique la dirección IP del sistema Guardium que controlará el S-TAP.
- Verifique que el directorio en el que va a instalar el S-TAP esté vacío o que no exista.

Procedimiento

1. Inicie una sesión en el servidor de base de datos mediante una cuenta de administrador del sistema.
2. Mediante el indicador de mandatos de Windows, vaya al directorio del instalador de S-TAP de Windows. Por ejemplo,

   ```
   cd c:\Windows-V10-r79771
   ```

   Debería encontrar un ejecutable setup.exe en el directorio del instalador.
3. Instale el S-TAP utilizando el ejecutable setup.exe con los parámetros adecuados. Por ejemplo,

   ```
   setup.exe -UNATTENDED -APPLIANCE 10.0.147.234 -TAPHOST 10.0.145.41
   ```

   - -UNATTENDED (obligatorio) invoca el instalador de la línea de mandatos.
   - -APPLIANCE especifica la dirección IP del sistema Guardium que controlará el S-TAP.
   - -TAPHOST (obligatorio) especifica la dirección IP del cliente donde se está instalando el S-TAP.

   Para ver una descripción completa del ejecutable de setup.exe y sus parámetros, consulte Referencia de la instalación desde la línea de mandatos de S-TAP de Windows

Qué hacer a continuación

Verifique que el S-TAP se está comunicando con el sistema Guardium; para ello, vaya a Gestionar > Supervisión de actividad > Control de S-TAP y revise el estado y la configuración de S-TAPs.

Tema principal: Instalación de un S-TAP en un servidor Windows
Referencia relacionada:
Referencia de la instalación desde la línea de mandatos de S-TAP de Windows

Referencia de la instalación desde la línea de mandatos de S-TAP de Windows

El instalador de línea de mandatos le permite crear scripts que resultan especialmente útiles para gestionar despliegues de gran tamaño. Esta referencia contiene los parámetros (cada uno con una breve descripción) que se pueden utilizar con en los scripts.

En una instalación de CLI, instale un S-TAP utilizando el ejecutable setup.exe con los parámetros adecuados y en este formato:

Setup.exe -PARAMETER valor

No utilice signos "=" para asignar valores a los parámetros. La única vez que se utiliza "=" es cuando se desea añadir un parámetro a la sección TAP del archivo guard_tap.ini directamente tal como se ha escrito en la línea de mandatos.

Si desea añadir parámetros adicionales que no se hayan especificado aquí, pero que se necesitan en el archivo guard_tap.ini, puede añadir la sección [TAP] especificando el parámetro y el valor con un signo =, por ejemplo:

setup.exe -UNATTENDED -INSTALLPATH "C:/Program Files/IBM/Windows S-TAP" -APPLIANCE 10.0.148.160 -TAPHOST 10.0.146.160 QRW_INSTALLED=0 QRW_DEFAULT_STATE=0

Importante: Los atributos UNATTENDED y TAPHOST son obligatorios.

Tabla 1. Parámetros aplicables a todos los instaladores .NET

Parámetro	Descripción
-UNATTENDED	Instalación silenciosa. (No necesita ningún valor)
-INSTALLPATH	Este es el directorio de instalación. La vía de acceso de instalación predeterminada es "C:/Program Files/IBM/Windows S-TAP"
-ENABLEGAM	Este parámetro habilita el servicio Guardium Agent Monitor (GAM).
-UNINSTALL	Desinstalación. No es necesario ningún valor.
-CUSTOMER	Para cambiar el nombre del cliente
-COMPANY	Para cambiar el nombre de la empresa
-SERVICEUSER	Para especificar el usuario bajo el que se ejecutará el servicio
-SERVICEPASSWORD	La contraseña del usuario

Tabla 2. Parámetros de S-TAP con el valor aplicable ON . Estos parámetros están activados de forma predeterminada con su valor establecido en ON. A menos que se indique lo contrario, si se establece para estos parámetros cualquier valor distinto de ON se desactiva el parámetro.

Parámetro	Descripción
-TCP	TCP_DRIVER_INSTALLED=1
-NMP	NAMED_PIPE_DRIVER_INSTALLED=1
-DB2SHMEM	DB2_TAP_INSTALLED=1
-DB2EXIT	DB2_EXIT_DRIVER_INSTALLED=1
-FAM	FSM_DRIVER_INSTALLED=1
-ORACLEPLUGIN	ORA_DRIVER_INSALLED=1
-MSPLUGIN	KRB_MSSQL_DRIVER_INSTALLED=2 (sólo si se ha establecido originalmente en 0 o para una instalación limpia)

Tabla 3. Otros parámetros de S-TAP

Parámetro	Descripción
-NOAUTODISCOVERY	Para impedir que el se ejecute el descubrimiento automático durante la instalación. No es necesario ningún valor.
-ENABLEGAM	Este parámetro habilita el servicio Guardium Agent Monitor (GAM).
-START	Se utiliza para iniciar el servicio después de la instalación. Atención: Este parámetro toma on como valor predeterminado y sólo se puede inhabilitar estableciendo su valor en 0. Cualquier valor distinto de 0 hace que este parámetro se active.
-TAPHOST	Es la IP local/del cliente. Este parámetro es obligatorio para una instalación desatendida.
-APPLIANCE	Es la IP de SQLGUARD. Puede configurar varios dispositivos simplemente especificando este parámetro con un nuevo valor varias veces.
-LOAD-BALANCER-IP	Es la IP del CM que permite que se habilite el equilibrador de carga
-LB-APP-GROUP	Especifique un nombre de grupo de aplicaciones al que pertenece este STAP para el equilibrio de carga empresarial. Atención: Los nombres de grupo con espacios o caracteres especiales no reciben soporte.
-LB-MU-GROUP	Especifique un nombre de grupo de MU para el equilibrio de carga empresarial. Atención: Los nombres de grupo con espacios o caracteres especiales no reciben soporte.
-LB-NUM-MUS	Para especificar el número de MU que desea asignar

Tema principal: Instalación de un S-TAP en un servidor Windows

Actualización y eliminación de un S-TAP en Windows

Aprenda a actualizar o a eliminar un S-TAP en Windows.

Tema principal: Instalación de un S-TAP en un servidor Windows

Actualización de un S-TAP de Windows mediante la línea de mandatos

Acerca de esta tarea

Si se ha instalado una versión anterior de S-TAP de Windows, se puede realizar una actualización desde la línea de mandatos utilizando el programa de instalación.

Procedimiento

1. Inicie una sesión en el sistema servidor de base de datos mediante una cuenta de administrador del sistema.
2. Vaya al directorio que contiene el programa de instalación de S-TAP.
3. Ejecute el programa de instalación con las opciones siguientes: setup -UNATTENDED
   Atención: Algunos archivos del release anterior no se eliminarán completamente hasta el siguiente rearranque planificado.

Eliminación de un S-TAP de Windows mediante Agregar o quitar programas

Acerca de esta tarea

Este procedimiento eliminará el S-TAP instalado mientras se asegura que el archivo de configuración se guarda para utilizarlo en el futuro.

Procedimiento

1. Inicie una sesión en el sistema servidor de base de datos mediante una cuenta de administrador del sistema.
2. Copie el archivo de configuración de S-TAP actual en una ubicación segura (un directorio que no sea Guardium). Busque este archivo en C:Program Files (x86)\IBM\Windows S-TAP\Bin\guard_tap.ini.
3. En el panel de control Agregar o quitar programas, elimine GUARDIUM_STAP.
   Atención: Algunos archivos no se eliminarán por completo hasta el siguiente rearranque planificado.

Eliminación de un S-TAP de Windows mediante la línea de mandatos

Acerca de esta tarea

Este procedimiento eliminará el S-TAP instalado mientras se asegura que el archivo de configuración se guarda para utilizarlo en el futuro.

Procedimiento

1. Inicie una sesión en el sistema servidor de base de datos mediante una cuenta de administrador del sistema.
2. Copie el archivo de configuración de S-TAP actual en una ubicación segura (un directorio que no sea Guardium). Busque este archivo en C:Program Files (x86)\IBM\Windows S-TAP\Bin\guard_tap.ini.
3. Vaya al directorio que contiene el programa de instalación de S-TAP.
4. Ejecute el programa de instalación con las opciones siguientes: setup -UNINSTALL
   Atención: Algunos archivos no se eliminarán por completo hasta el siguiente rearranque planificado.

Instale el cliente de S-TAP en un servidor Linux, Solaris, AIX o HP-UX

Puede instalar el cliente de S-TAP en un servidor Linux, Solaris, AIX o HP-UX con: Guardium Installation Manager (GIM), el RPM, el instalador del shell o el instalador nativo. Utilice el método que mejor se adapte a sus necesidades.

Además de los métodos listados a continuación, al iniciar Guardium V.10.1.3, podrá activar de forma automática clientes de GIM, instalar S-TAP y empezar a supervisar el trafico de las bases de datos. Consulte Inicio rápido para desplegar agentes de supervisión

Cuando instala un cliente de S-TAP, el programa de instalación comprueba si existe el grupo de guardium. Si el grupo no existe, el programa de instalación lo crea. Si utiliza determinados componentes o características, como por ejemplo A-TAP o DB2 Exit, debe añadir usuarios a este grupo para garantizar su correcto funcionamiento. Estos requisitos se describen en las secciones relevantes.

S-TAP instala en /usr/local/guardium

En situaciones poco habituales podría necesitar ejecutar S-TAP como guardium (y no como root). Esto puede ocasionar otros problemas y sólo se debe utilizar cuando sea necesario. La ejecución de S-TAP como usuario de Guardium puede hacer que algunas bases de datos o protocolos dejen de funcionar debido a algunos de los niveles de permiso. Verifique que la vía de acceso a la base de datos o al archivo ejecutable tiene los permisos de lectura para el usuario de Guardium. En función del entorno, las limitaciones típicas son:

- El descubrimiento tiene una funcionalidad limitada
- Es posible que wait_for_db_exec no funcione. Para un clúster, compruebe la vía de acceso de la base de datos o el archivo exec para ver el permiso de lectura del usuario Guardium.
- Es posible que la base de datos en WPAR de AIX y zonas de Solaris no funcione; compruebe el permiso para acceder a la vía de acceso de instalación o al archivo exec
- Para Oracle BEQ, reinicie S-TAP después de iniciar o reiniciar la base de datos.
- Para la memoria compartida de Informix, reinicie S-TAP después de iniciar o reiniciar la base de datos.
- Para la memoria compartida de DB2,
  - Cuando ktap_fast_shmem se establece en 0, si shmctl falla debido a un problema de permisos, en la mayoría de los casos debería ejecutar S-TAP como root.
  - Cuando ktap_fast_shmem se establece en 1, si el segmento de memoria compartida tiene permiso de lectura por grupo, asegúrese de que la instancia de DB2 se ha añadido al grupo de usuarios (Guardium). En cada servidor sólo se puede dar soporte a un conjunto de configuraciones de DB2.
  - Si el segmento de memoria compartida tiene permiso de lectura por grupo solo por usuario de DB2, se tiene que ejecutar S-TAP como root. (Abra una sesión de memoria compartida de DB2, ejecute el mandato ipcs -ma y compruebe MODE en la salida).

- Elección de la configuración de S-TAP
  Seleccione su configuración de S-TAP según los datos que desee supervisar o bloquear. Es preferible utilizar las bibliotecas de salida por encima de cualquier otro mecanismo de supervisión. Si no puede utilizar una biblioteca de salida, K-TAP es la siguiente elección.
- Instalación del cliente S-TAP en servidores Linux, Solaris, AIX y HP-UX con GIM
  Guardium Installation Manager permite instalar el agente de S-TAP desde un dispositivo de Guardium autónomo o desde el Gestor central (CM) para planificar la instalación en una o varias bases de datos. Después de la instalación, puede gestionar todos los parámetros y supervisar los procesos que fueron instalados bajo su control. Si instala mediante uno de los otros métodos de instalación, con GIM se pueden modificar menos parámetros.
- Instalación y desinstalación de S-TAP en un servidor Linux, Solaris, AIX y HP-UX utilizando RPM
  S-TAP se puede instalar, desinstalar y actualizar en un servidor Linux mediante RPM. La ventaja de instalar mediante RPM es que instalará y mantendrá el S-TAP

con el mismo método que el utilizado para gestionar el resto del software en el servidor de base de datos.

- Instalación de STAP de Linux, Solaris, AIX y HP-UX utilizando el instalador de shell
  Utilice el instalador de shell, en la modalidad interactiva o no interactiva, para instalar el cliente de S-TAP en servidores de bases de datos Linux, Solaris, HPUX y AIX.
- Instalación y desinstalación de un S-TAP de Linux, Solaris, AIX y HP-UX con un instalador nativo
  El instalador nativo proporciona un shell para el instalador de shell. La única ventaja es que se garantiza que S-TAP se registra en el repositorio de activos del sistema operativo. Guardium no requiere este registro para la instalación de S-TAP, pero podría ser un requisito de su empresa. Utilice el instalador nativo solo cuando sea necesario.
- Desinstalación de S-TAP
  Lleve a cabo este procedimiento antes de instalar una nueva versión de S-TAP si desea guardar el archivo de configuración antiguo.
- Trabajar con K-TAP
- Obtención de información de Java o Perl
  Es posible que tenga que comprobar la versión de Java o Perl que se está utilizando en el servidor de datos.

Tema principal: Instalación de S-TAP

Elección de la configuración de S-TAP

Seleccione su configuración de S-TAP según los datos que desee supervisar o bloquear. Es preferible utilizar las bibliotecas de salida por encima de cualquier otro mecanismo de supervisión. Si no puede utilizar una biblioteca de salida, K-TAP es la siguiente elección.

Utilice esta tabla para identificar los mecanismos de supervisión que pueden realizar las operaciones que precise, por sistema operativo y base de datos. Por ejemplo, es posible que desee rastrear o realizar alguna o varias de las siguientes tareas:

- Sólo tráfico local
- Tráfico de red y local
- Memoria compartida
- Datos cifrados
- Supervisar y bloquear
- Solo supervisar

Esta tabla abarca las plataformas más comunes, los tipos de bases de datos y los protocolos soportados por los mecanismos de supervisión de Guardium. En la tabla se presentan directrices generales. Es posible que se dé soporte a otras combinaciones que no se presentan aquí. Algunas de las configuraciones soportadas que aquí se presentan pueden depender de configuraciones específicas. Póngase en contacto con el soporte al cliente para verificar la mejor configuración para sus necesidades específicas. Celdas vacías indican que la combinación no está soportada.

SO	Base de datos	Tráfico de red	Tráfico local	Tráfico cifrado	Memoria compartida	Kerberos	Bloqueo	Redacción	Cadena de UID
AIX	Oracle	K-TAP	K-TAP	A-TAP (ASO, SSL)		K-TAP	K-TAP, A-TAP	K-TAP	K-TAP
AIX	Sybase ASE	K-TAP	K-TAP	A-TAP (SSL)		K-TAP	K-TAP, A-TAP	K-TAP	K-TAP, A-TAP (Solo ATAP cuando se configura para IP reales)
AIX	Sybase IQ	K-TAP	K-TAP	A-TAP (solo descifra paquetes de inicio de sesión, no da soporte a TLS).	A-TAP		K-TAP, A-TAP	K-TAP	K-TAP
AIX	DB2	DB2 Exit, K-TAP	DB2 Exit, K-TAP	DB2 Exit	DB2 Exit, K-TAP	K-TAP	DB2 Exit, K-TAP	K-TAP	DB2 Exit, K-TAP
AIX	Informix	Informix Exit, K-TAP	Informix Exit, K-TAP	Informix Exit	Informix Exit, K-TAP		Informix Exit, K-TAP	Informix Exit, K-TAP	Informix Exit, K-TAP
HP-UX	Oracle	K-TAP	K-TAP	A-TAP (ASO, SSL)		K-TAP	K-TAP, A-TAP	K-TAP	K-TAP
HP-UX	Sybase ASE	K-TAP	K-TAP	A-TAP (Solo Sybase 15)			K-TAP, A-TAP	K-TAP	K-TAP, A-TAP (Solo ATAP cuando se configura para IP reales)
HP-UX	Sybase IQ	K-TAP	K-TAP				K-TAP	K-TAP	K-TAP
HP-UX	DB2	DB2 Exit, K-TAP	DB2 Exit, K-TAP	DB2 Exit	DB2 Exit, K-TAP	K-TAP	DB2 Exit, K-TAP	K-TAP	DB2 Exit, K-TAP
HP-UX	Informix	Informix Exit, K-TAP	Informix Exit, K-TAP	Informix Exit	Informix Exit, K-TAP		Informix Exit, K-TAP	Informix Exit, K-TAP	Informix Exit, K-TAP
Linux	DB2	DB2 Exit, K-TAP		DB2 Exit	DB2 Exit, A-TAP	K-TAP	DB2 Exit, K-TAP, A-TAP(ATAP solo con Linux 2.6.36 y superior)	K-TAP	DB2 Exit, K-TAP

SO	Base de datos	Tráfico de red	Tráfico local	Tráfico cifrado	Memoria compartida	Kerberos	Bloqueo	Redacción	Cadena de UID
Linux	Informix	Informix Exit, K-TAP	Informix Exit, K-TAP	Informix Exit	Informix Exit, A-TAP		Informix Exit, K-TAP, A-TAP(ATAP solo con Linux 2.6.36 y superior)	Informix Exit, K-TAP	Informix Exit, K-TAP
Linux	Oracle	K-TAP	K-TAP	A-TAP (ASO, SSL)		K-TAP	K-TAP, A-TAP(ATAP solo con Linux 2.6.36 y superior)	K-TAP	K-TAP
Linux	Postgres	K-TAP	K-TAP	A-TAP			K-TAP, A-TAP(ATAP solo con Linux 2.6.36 y superior)	K-TAP	K-TAP, A-TAP (Solo ATAP cuando se configura para IP reales)
Linux	Sybase IQ	K-TAP		A-TAP (solo x86_64)	A-TAP		K-TAP, A-TAP(ATAP solo con Linux 2.6.36 y superior)	K-TAP	K-TAP, A-TAP (Solo ATAP cuando se configura para IP reales)
Linux	Sybase ASE	K-TAP	K-TAP	A-TAP			K-TAP, A-TAP(ATAP solo con Linux 2.6.36 y superior)	K-TAP	K-TAP, A-TAP (Solo ATAP cuando se configura para IP reales)
Linux	MongoDB	K-TAP	K-TAP	A-TAP			K-TAP, A-TAP(ATAP solo con Linux 2.6.36 y superior)	K-TAP	K-TAP, A-TAP (Solo ATAP cuando se configura para IP reales)
Linux	Teradata	Teradata Exit, K-TAP		Teradata Exit, A-TAP			Teradata Exit, K-TAP, A-TAP(ATAP solo con Linux 2.6.36 y superior)	K-TAP	K-TAP, A-TAP (Solo ATAP cuando se configura para IP reales)
Linux	Netezza	K-TAP					K-TAP	K-TAP	K-TAP
Linux	Cassandra	K-TAP					K-TAP	K-TAP	K-TAP
Linux	SAP HANA	K-TAP					K-TAP	K-TAP	K-TAP
Linux	MySQL	K-TAP	K-TAP				K-TAP	K-TAP	K-TAP
Linux	MemSQL	K-TAP	K-TAP	K-TAP			K-TAP	K-TAP	K-TAP
Linux	Vertica	K-TAP	K-TAP				K-TAP	K-TAP	K-TAP
Linux	Hadoop (Cloudera / Hortonworks)	K-TAP, Cloudera Navigator, Hortonworks y Apache Ranger		Cloudera Navigator, Hortonworks y Apache Ranger			Hortonworks y Apache Ranger		K-TAP
Linux	Greenplum	K-TAP	K-TAP	A-TAP			K-TAP, A-TAP (solo Linux 2.6.36 y superior)	K-TAP	K-TAP
Linux	MariaDB	K-TAP	K-TAP				K-TAP	K-TAP	K-TAP
Linux	Aster	K-TAP	K-TAP				K-TAP	K-TAP	K-TAP
Linux	Couch	K-TAP					K-TAP	K-TAP	K-TAP
Linux	Hive	K-TAP					K-TAP	K-TAP	K-TAP
Linux	Accumulo	K-TAP					K-TAP	K-TAP	K-TAP
Linux	Impala	K-TAP					K-TAP	K-TAP	K-TAP
Linux	Hue	K-TAP	K-TAP				K-TAP	K-TAP	K-TAP
Linux	WebHDFS	K-TAP					K-TAP	K-TAP	K-TAP
Linux	Solar	K-TAP					K-TAP	K-TAP	K-TAP
Solaris	Oracle	K-TAP	K-TAP	A-TAP (ASO, SSL)		K-TAP	K-TAP, A-TAP	K-TAP	K-TAP

SO	Base de datos	Tráfico de red	Tráfico local	Tráfico cifrado	Memoria compartida	Kerberos	Bloqueo	Redacción	Cadena de UID
Solaris	Sybase ASE	K-TAP	K-TAP	A-TAP (solo Sparc)		K-TAP	K-TAP, A-TAP	K-TAP	K-TAP, A-TAP (Solo ATAP cuando se configura para IP reales)
Solaris	Postgres	K-TAP	K-TAP	A-TAP (9.3 y superior)			K-TAP, A-TAP	K-TAP	K-TAP, A-TAP (Solo ATAP cuando se configura para IP reales)
Solaris	Sybase IQ	K-TAP	K-TAP				K-TAP	K-TAP	K-TAP
Solaris	DB2	DB2 Exit, K-TAP	DB2 Exit, K-TAP	DB2 Exit	DB2 Exit, K-TAP	K-TAP	DB2 Exit, K-TAP	K-TAP	DB2 Exit, K-TAP
Solaris	Informix	Informix ExitExit, K-TAP	Informix Exit, K-TAP	Informix Exit	Informix Exit, K-TAP		Informix Exit, K-TAP	Informix Exit, K-TAP	Informix Exit, K-TAP

Tema principal: Instale el cliente de S-TAP en un servidor Linux, Solaris, AIX o HP-UX

Instalación del cliente S-TAP en servidores Linux, Solaris, AIX y HP-UX con GIM

Guardium Installation Manager permite instalar el agente de S-TAP desde un dispositivo de Guardium autónomo o desde el Gestor central (CM) para planificar la instalación en una o varias bases de datos. Después de la instalación, puede gestionar todos los parámetros y supervisar los procesos que fueron instalados bajo su control. Si instala mediante uno de los otros métodos de instalación, con GIM se pueden modificar menos parámetros.

Acerca de esta tarea

Procedimiento

1. Obtenga la dirección IP del servidor de base de datos en el que está instalando S-TAP. Si se utilizan IP virtuales, anótelas también (tendrá que configurarlas más adelante, cuando complete la configuración).
2. Si está realizando la instalación en el Gestor central (CM), identifique la dirección IP del recopilador que controlará este S-TAP, y al que este S-TAP informará.
3. Verifica la conectividad entre el servidor de bases de datos y el recopilador. En la base de datos, especifique nmap -p <puerto> <dirección_ip>. Por ejemplo, para comprobar que el puerto 16018 (el puerto que Guardium utiliza para TLS) es accesible en la dirección IP 192.168.3.104, especifique el mandato nmap -p 16018 192.168.3.104
   La salida típica es parecida a la siguiente:
   ```
   Starting nmap V. 3.00 Interesting ports on g4.guardium.com (192.168.3.104): Port State Service 16018/tcp open unknown
   ```
4. Verifique que el cliente GIM está instalado en el servidor de base de datos. Consulte Instalación del cliente GIM en un servidor UNIX.
5. Obtenga el script instalador de S-TAP correcto. El nombre del script identifica el sistema operativo del servidor de base de datos.
6. Actualice el módulo de S-TAP relevante para el dispositivo de Guardium Installation Manager.
   a. Vaya a Gestionar > Instalación de módulo > Subir módulos.
   b. Pulse Elegir archivo y seleccione el módulo de S-TAP que desea instalar.
   c. Pulse Subir para subir el módulo para el dispositivo. El módulo aparece en la tabla Importar módulos subidos.
   d. En la tabla Importar módulos subidos, marque el recuadro de selección situado junto al módulo de S-TAP que desea instalar. Se importa el módulo que pasa a estar disponible para la instalación. Se restablece la página Subir módulos y la tabla Importar módulos subidos aparece ahora vacía.
7. Seleccione una o varias bases de datos en las que instalar el S-TAP.
   a. Vaya a Gestionar > Instalación de módulo > Configuración por cliente (Antiguo).
   b. En la página Criterios de búsqueda de cliente, especifique criterios de búsqueda para las bases de datos donde desea instalar el S-TAP y, a continuación, pulse Buscar para continuar. Busque bases de datos con cualquier combinación de los criterios de búsqueda siguientes.
      - Seleccionar un grupo de clientes.
      - Buscar por nombre de host, dirección IP o sistema operativo de cliente.
      - Deje todos los campos de criterios de búsqueda vacíos y pulse Buscar para recuperar con una lista de todos los clientes disponibles.
   c. En la página Clientes, seleccione los recuadros de selección junto a los clientes en los que desea instalar el S-TAP y, a continuación, pulse Siguiente.
8. Seleccione y configure los parámetros de S-TAP antes de realizar la instalación en los sistemas cliente.
   a. Desde la tabla Módulos en la página Módulos comunes, seleccione el módulo S-TAP para la instalación.
      - Utilice los recuadros de selección Visualizar las últimas versiones y Visualizar solo lotes para filtrar la lista de módulos disponibles.
      - Utilice la tabla Estado de módulo para revisar la información sobre el módulo seleccionado en los clientes de destino.
   b. Pulse Siguiente.
   c. En la página Parámetros de módulo de cliente, puede especificar parámetros para un grupo de bases de datos o para bases de datos individuales.
      - Aplique los mismos valores de parámetro a varias bases de datos: Especifique los valores en los campos Parámetros de módulo comunes, pulse los recuadros de selección junto a las bases de datos en las tablas Parámetros de módulo de cliente y, a continuación, pulse Aplicar a seleccionados.
      - Para aplicar parámetros exclusivos a clientes individuales, especifique los valores de Parámetros del módulo de cliente de la tabla y pulse Aplicar a los clientes.

      Atención:

      Estos parámetros son obligatorios:

      - KTAP_LIVE_UPDATE: Especifique Y para habilitar la actualización de KTAP sin la necesidad de rearrancar el servidor
      - STAP_TAP_IP: Dirección IP o FQDN del nodo o servidor de base de datos en el que el STAP está siendo instalado (equivale al parámetro de línea de mandatos -taphost). Si no se especifica, se utiliza el valor GIM_CLIENT_IP.
      - STAP_SQLGUARD_IP: Dirección IP o FQDN del recopilador primario con el que el STAP se comunica (equivale al parámetro de línea de mandatos -appliance). Si no se especifica, entonces se utiliza el valor GIM_URL.
      - Solo para Linux: KTAP_ALLOW_MODULE_COMBOS. Especifique Y (el valor predeterminado es N). Si el lote no tiene una coincidencia de kernel exacta, instala la que más se aproxima. Si el K-TAP no se puede instalar o no se inicia, se visualiza pregunta al usuario si desea continuar con la instalación.
   d. Aplique los parámetros a los clientes seleccionados pulsando Aplicar a cliente.
9. Instale el S-TAP:

a. Verifique que la base de datos está seleccionado en la tabla Parámetros de módulo de cliente.
b. Pulse Instalar/Actualizar, en la parte inferior de la ventana.
c. En un Gestor central (CM), en el área Fecha de planificación, proporcione una fecha u hora en la que comenzar la instalación y, a continuación pulse Aplicar. Para empezar la instalación inmediatamente, utilice el valor `ahora` en el campo Fecha de planificación.

Qué hacer a continuación

Verifique el estado de S-TAP:

- Consulte el estado de instalación del módulo en el informe Gestionar > Informes > Gestión de instalación > Estado de los clientes de GIM
- Supervise la instalación de los clientes de Guardium navegando a Gestionar > Instalación de módulo > Configuración por cliente (Antiguo). Pulse Buscar y, a continuación, pulse el junto al S-TAP.
- Verifique que la fila de S-TAP tiene un estado verde (primera columna) en Supervisar > Mantenimiento > Registros de S-TAP > Estado de S-TAP

Tema principal: Instale el cliente de S-TAP en un servidor Linux, Solaris, AIX o HP-UX
Conceptos relacionados:
Guardium Installation Manager

Instalación y desinstalación de S-TAP en un servidor Linux, Solaris, AIX y HP-UX utilizando RPM

S-TAP se puede instalar, desinstalar y actualizar en un servidor Linux mediante RPM. La ventaja de instalar mediante RPM es que instalará y mantendrá el S-TAP con el mismo método que el utilizado para gestionar el resto del software en el servidor de base de datos.

Acerca de esta tarea

Los nombres de RPM tienen el formato: guard-stap-10.1.0.89165-1-rhel-6-linux-x86_64.x86_64.rpm, donde los tres primeros números son el número de release de STAP (10.1.0, 10.1.2, etc) y el cuarto número es la revisión de código (89165). El número que aparece inmediatamente después es la iteración del paquete, que se incrementaría en el caso de añadir módulos KTAP al RPM.

Hay un único RPM para los S-TAP de 32 bits y dos RPM para los S-TAP de 64 bits, de forma que el S-TAP de 64 bits no tiene una dependencia de las bibliotecas de 32 bits si no se necesitan bibliotecas de salida de 32 bits. El RPM adicional se parece a guard-stap-32bit-exit-libs-10.1.0.89165-1-rhel-6-linux-x86_64.x86_64.rpm y depende del RPM principal.

De forma predeterminada, el proceso de instalación comprueba el kernel de Linux para determinar si se ha creado un módulo K-TAP para que funcione con dicho kernel. Si existe, se instala (establece ktap_installed = 1). Si no hay ninguno, no se instala K-TAP a menos que haya habilitado la flexibilidad de carga, que ayuda a la instalación de módulos compilados actualmente cuando no existe una coincidencia exacta. Cuando se habilita la flexibilidad de carga, se intenta compilar un K-TAP para que coincida con su kernel de Linux.

RPM instala S-TAP en /opt/guardium; no es posible cambiar esta ubicación. tap_ip se establece automáticamente en el nombre de host del sistema. sqlguard_ip se establece en 127.0.0.1 como marcador para una configuración correcta. Complete la configuración después de la instalación, tal como se describe en este procedimiento.

Procedimiento

1. Obtenga la dirección IP del servidor de base de datos en el que está instalando S-TAP. Si se utilizan IP virtuales, anótelas también (tendrá que configurarlas más adelante, cuando complete la configuración).
2. Identifique la dirección IP del recopilador que controlará esta instancia de S-TAP y a la que informará esta instancia de S-TAP.
3. Verifica la conectividad entre el servidor de bases de datos y el recopilador. En la base de datos, especifique nmap -p <puerto> <dirección_ip>. Por ejemplo, para comprobar que el puerto 16018 (el puerto que Guardium utiliza para TLS) es accesible en la dirección IP 192.168.3.104, especifique el mandato
   nmap -p 16018 192.168.3.104
   La salida típica es parecida a la siguiente:
   `Starting nmap V. 3.00 Interesting ports on g4.guardium.com (192.168.3.104): Port State Service 16018/tcp open unknown`
4. Obtenga el script instalador de S-TAP correcto. El nombre del script identifica el sistema operativo del servidor de base de datos.
5. Descomprima el paquete y copie los RPM en /tmp del servidor de bases de datos.
6. Para habilitar la flexibilidad de carga, establezca la variable de entorno de Linux `NI_ALLOW_MODULE_COMBOS="Y"`.
7. Instale el RPM.
   a. Ejecute el mandato: `rpm -i <RPM_NAME>`

      Se instala el S-TAP.

   b. Complete la configuración ejecutando el script `guard-config-update` utilizando los parámetros descritos en 9.
   El instalador de shell de S-TAP no instala si ya hay un RPM instalado (impidiendo una doble instalación).
8. Para actualizar, copie el paquete RPM en /opt/guardium y ejecute el mandato: `rpm -U <RPM_NAME>`
9. Para configurar o actualizar: Inicie una sesión en el sistema como `root`, cambie al directorio /opt/guardium y ejecute el script `guard-config-update` mediante las correspondientes [opciones] y [acciones] desde las siguientes listas:
   Nota: Los valores prestablecidos se deben ubicar al inicio del mandato. Los valores prestablecidos al final originarán una compilación anómala. La utilización de valores preestablecidos y un archivo como argumento funciona bien.

[--stap-dir]	Directorio de instalación de STAP si no es el predeterminado (predeterminado:/usr/local/guardium)
[--set-tap-ip [IP o nombre_host]]	Establece tap_ip en el archivo de configuración de STAP /usr/local/guardium/guard_stap/guard_tap.ini (predeterminado:rh5u9x64t.guard.swg.usma.ibm.com)
[--set-sqlguard-ip [IP o nombre_host]]	Establece sqlguard_ip en la sección SQLGuard_0 en el archivo de configuración de STAP /usr/local/guardium/guard_stap/guard_tap.ini (predeterminado: 127.0.0.1)
[--add-sqlguard [ID] [IP o nombre_host]] (Guardium v10.1.4 y superior)	Añade la sección SQLGuard_ID al archivo de configuración de STAP /usr/local/guardium/guard_stap/guard_tap.ini
[--remove-sqlguard [ID]]	Elimina la sección SQLGuard_ID del archivo de configuración de STAP /usr/local/guardium/guard_stap/guard_tap.ini

(Guardium v10.1.4 y superior)	
[--modify-sqlguard [ID] [parámetro] [valor]] (Guardium v10.1.4 y superior)	Establece el parámetro de la sección SQLGuard_ID con el valor en el archivo de configuración de STAP /usr/local/guardium/guard_stap/guard_tap.ini. Parámetros: sqlguard_ip Dirección IP o nombre de host de la unidad de SQLGuard sqlguard_port Puerto utilizado para conectarse a la unidad de SQLGuard (predeterminado: 16016) primary Orden de preferencia (1 es el de mayor preferencia) num_main_thread Número de conexiones principales para utilizar para este SQLGuard. Se utiliza junto conparticipate_in_load_balancing = { 1, 4 } (predeterminado: 1) connection_pool_size Número de conexiones de datos por conexión principal con la unidad de SQLGuard (valor predeterminado: 0)
[--modify-tap [parámetro] [valor]] (Actualizado en Guardium v10.1.4)	Establece el parámetro de la sección TAP con el valor en el archivo de configuración de STAP /usr/local/guardium/guard_stap/guard_tap.ini. Parámetros: tap_debug_output_level Establece el nivel de depuración (debe ser un entero >= 0 y distinto de 2 y de 3). participate_in_load_balancing Establece la participación en el equilibrio de carga (debe ser un entero >= 0 y <= 4) use_tls Habilita TLS [0, 1] failover_tls Sustitución por anomalía de conexiones TLS a no TLS [0, 1] hunter_trace Habilita la creación de informes de cadena de UID [0, 1] buffer_file_size Tamaño del archivo de almacenamiento intermedio en MB alternate_ips Lista separada por comas de direcciones de IP/nombres de host alternativos para STAP firewall_installed Habilita el cortafuegos [0, 1] firewall_fail_close Acción que se emprenderá cuando no haya un veredicto (es decir, no se pueda acceder a SQLGuard o se supere el tiempo de espera) [0 : no hacer nada, 1 : bloquear conexión] firewall_default_state Establece el estado predeterminado [0 : no vigilado, 1 : vigilado] firewall_timeout Establece el tiempo de espera del cortafuegos en segundos firewall_force_watch Lista separada por comas de direcciones de IP/máscaras que se deben vigilar aunque firewall_default_state=0 firewall_force_unwatch Lista separada por comas de direcciones IP/máscaras que no se deben vigilar incluso cuando firewall_default_state=1
[--help-config [option]]	Mostrar información sobre una opción en el ini, si está disponible (mostrar todas las disponibles si no se especifica)
[--set-flexload [0 or 1]]	Habilita o inhabilita la carga flexible de KTAP
[--retry-ktap-load]	Volver a intentar una carga de KTAP (útil después de instalar paquetes de dispositivos, de actualizar tras una solicitud de KTAP o de cambiar la carga de flexible; reinicia automáticamente STAP)
[--discover-ies]	Ejecutar el descubrimiento y sustituir todos los motores de inspección (IE) por los descubiertos
[--stop [service]]	Detiene el servicio temporalmente (los servicios Solaris e inittab tratan este valor como una inhabilitación permanente, no se inicia de forma automática al volver arrancar hasta que se vuelva a habilitar)
[--start [service]]	Inicia el servicio (stap, tee o supervisor) si aún no se está ejecutando (implica habilitar)
[--restart [service]]	Reinicia el servicio (stap, tee o supervisor) si aún no se está ejecutando
[--disable [service]]	Impide ejecutar de nuevo el servicio (stap, tee o supervisor)
[--enable [service]]	Configura el servicio (stap, tee o supervisor) para un inicio automático
[--status]	Muestra qué servicios se han iniciado y están configurados para que se inicien automáticamente

10. Para desinstalar:
    a. Para obtener el nombre del RPM, ejecute: `rpm -qa | grep guard_stap`

b. Ejecute `rpm -e <RPM_NAME>`

Después de desinstalar, el directorio /opt/guardium sigue existiendo, pero solo debería contener /opt/guardium/guard_stap/guard_tap.ini.rpmsave y /opt/guardium/rpm_logs

Qué hacer a continuación

Verificar estado de S-TAP:

- Verifique que la fila de S-TAP tiene un estado verde (primera columna) en Supervisar > Mantenimiento > Registros de S-TAP > Estado de S-TAP
- Verifique desde la base de datos que el STAP se está ejecutando y que el KTAP está cargado (si ha instalado un KTAP)

Tema principal: Instale el cliente de S-TAP en un servidor Linux, Solaris, AIX o HP-UX

Instalación de STAP de Linux, Solaris, AIX y HP-UX utilizando el instalador de shell

Utilice el instalador de shell, en la modalidad interactiva o no interactiva, para instalar el cliente de S-TAP en servidores de bases de datos Linux, Solaris, HPUX y AIX.

Acerca de esta tarea

La modalidad interactiva es una forma fácil de instalar y desinstalar, pero debe ejecutarse individualmente en cada sistema. Proporciona un sistema de validación en cada paso, lo que significa menos probabilidades de errores. Resulta útil para despliegues pequeños o siempre que se necesite una experiencia guiada de instalación paso a paso. En la modalidad no interactiva, puede instalar varios S-TAP con un script, lo que es especialmente útil para gestionar grandes despliegues.

Si alguna etapa de la instalación falla, deshaga todos los pasos hasta ese punto. No deje las instancias de S-TAP parcialmente instalado.

El nombre del paquete de S-TAP tiene el formato: guard-stap-guard-10.0.0_r79927_1-rhel-5-linux-x86_64.sh, donde 10.0.0 es el número de release y r79927 es el número de revisión.

Se recomienda la modalidad interactiva para S-TAP individuales. El sistema solicita la configuración básica, y verifica la entradas de forma inmediata, por lo que no hay errores. De forma predeterminada, K-TAP se instala automáticamente durante la instalación del S-TAP. El instalador de S-TAP comprueba si éste está disponible para la versión del kernel. Si el proceso de instalación no encuentra un K-TAP coincidente, intenta crear uno para que coincida con el kernel de Linux. Si el K-TAP no se puede instalar o no se inicia, se visualiza pregunta al usuario si desea continuar con la instalación.

Utilice la modalidad no interactiva para instalar en varias bases de datos varios sistemas ejecutando un único mandato, utilizando el parámetro tapfile, --tapfile <vía a archivo ini>, y un archivo de configuración asociado que especifique las bases de datos y sus detalles. Considere utilizar GIM en lugar de la modalidad no interactiva.

Procedimiento

1. Obtenga la dirección IP del servidor de base de datos en el que está instalando S-TAP. Si se utilizan IP virtuales, anótelas también (tendrá que configurarlas más adelante, cuando complete la configuración).
2. Identifique la dirección IP del recopilador que controlará esta instancia de S-TAP y a la que informará esta instancia de S-TAP.
3. Verifica la conectividad entre el servidor de bases de datos y el recopilador. En la base de datos, especifique nmap -p <puerto> <dirección_ip>. Por ejemplo, para comprobar que el puerto 16018 (el puerto que Guardium utiliza para TLS) es accesible en la dirección IP 192.168.3.104, especifique el mandato
   nmap -p 16018 192.168.3.104
   La salida típica es parecida a la siguiente:
   `Starting nmap V. 3.00 Interesting ports on g4.guardium.com (192.168.3.104): Port State Service 16018/tcp open unknown`
4. Obtenga el script instalador de S-TAP correcto. El nombre del script identifica el sistema operativo del servidor de base de datos.
5. Inicie la sesión en el servidor de bases de datos utilizando la cuenta `root`.
6. Designe un directorio de instalación y verifique que tiene suficiente espacio en disco, aproximadamente un total de 400 MB - 500 MB.
7. Copie el .tgz de S-TAP en el disco local en el servidor de bases de datos, habitualmente en /tmp.
8. Para una instalación típica en modalidad no interactiva, especifique:

   ```
   ./guard-stap-guard-<número release>_<número versión>_1-rhel-5-linux-x86_64.sh -- --ni -k --dir <dir_instalación_guardium>
     --ktap_allow_module_combos   --tapip <ip_tap o nombre_host>  --sqlguardip < ip_sqlguard o nombre_host>
   ```

   Nota: El instalador del S-TAP incluye todos los módulos específicos posibles para los distintos kernels de Linux. En casos raros, el paquete S-TAP no tiene el módulo K-TAP adecuado. En este caso, copie el módulo K-TAP en /tmp e instale con estos mandatos. El archivo del módulo K-TAP se copia en el directorio de instalación de S-TAP durante la instalación.

   ```
   ./guard-stap-guard-10.0.0_r79927_1-rhel-5-linux-x86_64.sh --
   --modules /tmp/modules-guard-10.0.0_r79927_1.tgz"
   ```

9. Para la modalidad interactiva
   a. Especifique: `./guard-stap-guard-<número release>_<número revisión>_1-rhel-5-linux-x86_64.sh`
   b. Responda a la notificación legal y a otras solicitudes, según indique el programa de instalación. Le sugerimos que acepte todos los valores predeterminados que se proporcionan.
   c. Cuando se le solicite la dirección IP del sistema Guardium, especifique la dirección IP del dispositivo con el que se debe comunicar este S-TAP.
   d. Cuando se le solicite la dirección IP del host de tap, especifique la dirección IP de la base de datos.
   e. En la solicitud del instalador para el nombre de usuario (root o guardium), seleccione `root`. En casos excepcionales, tendrá que ejecutar el S-TAP como Guardium. Esto puede ocasionar otros problemas y sólo se debe utilizar cuando sea absolutamente necesario.
   f. El instalador solicita cambios en el archivo de parámetros. Generalmente no es necesario editar el archivo, ya que puede establecer los valores de otros parámetros desde la interfaz de usuario de Guardium. Si decide editar el archivo de configuración, utilice el mandato :wq para guardar el archivo y salir. El programa de instalación verifica los valores de parámetro que ha establecido. Si son correctos, continúa con las siguientes solicitudes. De lo contrario, corrija los parámetros erróneos y vuelva a guardar el archivo.
   g. Solo para AIX : reinicie el servicio de base de datos y el de escucha. Todos los demás pueden saltarse este paso.
10. Complete la configuración de S-TAP desde la interfaz de usuario. Consulte Configuración de S-TAP desde la GUI.
11. Una vez instalado S-TAP, para las instancias de base de datos que A-TAP tiene que supervisar, añada el usuario de base de datos al grupo Guardium. Este grupo lo crea el instalador de S-TAP y el administrador del sistema puede añadir usuarios mediante el programa de utilidad usermod.
    A continuación se muestra un ejemplo, donde Oracle es el ID del usuario del sistema operativo para la base de datos Oracle y sybase15 es el ID del usuario del sistema operativo para la base de datos Sybase 15:

```
usermod -a -G guardium oracle
usermod -a -G guardium sybase15
```

Qué hacer a continuación

Verificar estado de S-TAP:

- Consulte el estado de instalación del módulo en el informe Gestionar > Informes > Gestión de instalación > Estado de los clientes de GIM
- Supervise la instalación de S-TAP en la tabla Estado de módulo en la pantalla Módulos comunes.
- Verifique que la fila de S-TAP tiene un estado verde (primera columna) en Supervisar > Mantenimiento > Registros de S-TAP > Estado de S-TAP
- Verifique desde la base de datos que el STAP se está ejecutando y que el KTAP está cargado (si ha instalado un KTAP)

- Parámetros de script de instalación de STAP para UNIX

Tema principal: Instale el cliente de S-TAP en un servidor Linux, Solaris, AIX o HP-UX

Parámetros de script de instalación de STAP para UNIX

Sintaxis de la instalación desde la línea de mandatos

uso: guard-stap-setup [opciones]

[--ni] - Instalación no interactiva

[-k | -p] - Instalación con Ktap o Pcap

[--ni] - Instalación no interactiva

[--ignore-compat] - Ignorar comprobación de compatibilidad de script

[-k | -t | -p] - Instalar con Ktap, Tee o Pcap

[-u] - Actualizar si se encuentra una instalación anterior

[--user | --root] - Ejecutar stap como usuario o root

[--userinst | --rootinst] - Instalar stap como usuario o root

[--overwrite-existing] - Sobrescribir instalación existente si se encuentra

[--tls force | failover | none] - Valor de TLS de Stap

[--dir <dir>] - Directorio de instalación de Stap

[--tapfile <file>] - Archivo de valores de Stap a utilizar para la instalación

[--ipfile <file>] - Archivo que especifica la IP de tap y la IP de sqlguard

[--tapip <tapip>] - La IP de la stap de la máquina en la que se está instalando

[--sqlguardip <sqlguardip>] - La IP de la gmachine con la que este stap se debe comunicar

[--presets <file> | <preset-options>] - Leer valores de instalación o escribirlos en un archivo

[--no-discovery] - No utilizar el programa de utilidad de descubrimiento para configurar los motores de inspección

[--load-balancer-ip <load_balancer_ip>] - La IP del equilibrador de carga que debe utilizar este stap

[--lb-app-group <app_group>] - Grupo de aplicaciones al que este stap pertenece
Atención: No se permiten grupos del equilibrador de carga empresarial con espacios o caracteres especiales.

[--lb-mu-group <mu_group>] - Grupo de unidades gestionadas al que este stap pertenece. También se debe especificar el grupo de aplicaciones que lo va a utilizar.

[--lb-num-mus <number_of_mus>] - Número de unidades gestionadas que debe asignar el equilibrador de carga para este stap.

[--modules <module-bundles>] - Especificar un lote de módulos de Ktap externo

[--ktap_allow_module_combos] - Permitir una coincidencia de kernel inexacta para cargar ktap

[--load-balancer-ip <load_balancer_ip>] - La IP del equilibrador de carga que debe utilizar este stap

[--lb-app-group <app_group>] - Grupo de aplicaciones al que este stap pertenece para el equilibrio de carga empresarial.

[--lb-mu-group <mu_group>] - Grupo de unidades gestionadas al que este stap pertenece para el equilibrio de carga empresarial. También se debe especificar el grupo de aplicaciones que lo va a utilizar.
Atención: Los nombres de grupo con espacios o caracteres especiales no reciben soporte.

[--lb-num-mus <number_of_mus>] - Número de unidades gestionadas que debe asignar el equilibrador de carga para este stap.

[--modules <module-bundles>] - Especifica un lote de módulos de Ktap externo

Tema principal: Instalación de STAP de Linux, Solaris, AIX y HP-UX utilizando el instalador de shell

Instalación y desinstalación de un S-TAP de Linux, Solaris, AIX y HP-UX con un instalador nativo

El instalador nativo proporciona un shell para el instalador de shell. La única ventaja es que se garantiza que S-TAP se registra en el repositorio de activos del sistema operativo. Guardium no requiere este registro para la instalación de S-TAP, pero podría ser un requisito de su empresa. Utilice el instalador nativo solo cuando sea necesario.

Un instalador nativo asegura que S-TAP está registrado en el repositorio de activos del sistema operativo. Guardium no requiere este registro para la instalación de S-TAP, pero podría ser un requisito de su empresa. Hay un instalador nativo independiente para cada tipo de sistema operativo.

- Instalación y desinstalación de S-TAP con el instalador nativo de AIX
- Instalación y desinstalación de S-TAP con un instalador nativo HP-UX
- Instalación y desinstalación de S-TAP con el instalador nativo de Solaris

Tema principal: Instale el cliente de S-TAP en un servidor Linux, Solaris, AIX o HP-UX

Instalación y desinstalación de S-TAP con el instalador nativo de AIX

Procedimiento

1. Obtenga la dirección IP del servidor de base de datos en el que está instalando S-TAP. Si se utilizan IP virtuales, anótelas también (tendrá que configurarlas más adelante, cuando complete la configuración).
2. Identifique la dirección IP del recopilador que controlará esta instancia de S-TAP y a la que informará esta instancia de S-TAP.
3. Verifica la conectividad entre el servidor de bases de datos y el recopilador. En la base de datos, especifique nmap -p <puerto> <dirección_ip>. Por ejemplo, para comprobar que el puerto 16018 (el puerto que Guardium utiliza para TLS) es accesible en la dirección IP 192.168.3.104, especifique el mandato
   nmap -p 16018 192.168.3.104
   La salida típica es parecida a la siguiente:
   ```
   Starting nmap V. 3.00 Interesting ports on g4.guardium.com (192.168.3.104): Port State Service 16018/tcp open unknown
   ```
4. Localice el archivo del instalador nativo adecuado (archivo .bff) en el DVD de instalación de Guardium S-TAP para su versión de AIX.
5. Especifique el mandato siguiente en un servidor limpio (sin instalación previa de S-TAP) para extraer el instalador de shell para AIX, sustituyendo el nombre de archivo adecuado por el archivo .bff apropiado:

   ```
   installp -aX -d/var/tmp<filename> SqlGuardInstaller
   Ejemplo:
   installp -aX -d/var/tmp/guard-stap-guard-8.0.00rc1_r20934_1-aix-5.2-aix-powerpc.bff SqlGuardInstaller
   ```

   El instalador de shell que se extrae, denominado guardium, está bajo /usr/local.

6. Continúe en el Paso 6 del procedimiento de instalación, ejecutando el script de instalación generado en lugar del script de instalación predeterminado para la versión del sistema operativo.

Tema principal: Instalación y desinstalación de un S-TAP de Linux, Solaris, AIX y HP-UX con un instalador nativo

Eliminación del S-TAP de AIX mediante el instalador nativo

Procedimiento

Para eliminar la instancia de S-TAP de AIX mediante el instalador nativo:

```
/usr/lib/instl/sm_inst installp_cmd -u -f 'filename'
```

Ejemplo

```
/usr/lib/instl/sm_inst installp_cmd -u -f'SqlGuardInstaller'
```

Instalación y desinstalación de S-TAP con un instalador nativo HP-UX

Acerca de esta tarea

Procedimiento

1. Obtenga la dirección IP del servidor de base de datos en el que está instalando S-TAP. Si se utilizan IP virtuales, anótelas también (tendrá que configurarlas más adelante, cuando complete la configuración).
2. Identifique la dirección IP del recopilador que controlará esta instancia de S-TAP y a la que informará esta instancia de S-TAP.
3. Verifica la conectividad entre el servidor de bases de datos y el recopilador. En la base de datos, especifique nmap -p <puerto> <dirección_ip>. Por ejemplo, para comprobar que el puerto 16018 (el puerto que Guardium utiliza para TLS) es accesible en la dirección IP 192.168.3.104, especifique el mandato
   nmap -p 16018 192.168.3.104
   La salida típica es parecida a la siguiente:
   ```
   Starting nmap V. 3.00 Interesting ports on g4.guardium.com (192.168.3.104): Port State Service 16018/tcp open unknown
   ```
4. Localice el archivo del instalador nativo adecuado (archivo .depot.gz) en el DVD de instalación de Guardium S-TAP para su versión de HPUX.
5. Extraiga el archivo con

   ```
   gzip -d <filename>.depot.gz
   ```

6. Escriba el mandato swinstall del siguiente modo, especificando el nombre del archivo seleccionado (el archivo adecuado del instalador nativo) y el nombre de host de su servidor de base de datos. Este mandato inicia un programa interactivo. Siga las indicaciones y utilice los controles adecuados para instalar el programa de instalación de S-TAP adecuado (archivo .sh), que se encuentra en /var/spool/sw/var/tmp.

   ```
   swinstall -s /var/tmp/<filename>.depot @ ,hostname>:/var/spool/sw
   ```

7. Continúe en el Paso 6 del procedimiento de instalación, ejecutando el script de instalación generado en lugar del script de instalación predeterminado para la versión del sistema operativo.

Tema principal: Instalación y desinstalación de un S-TAP de Linux, Solaris, AIX y HP-UX con un instalador nativo

Eliminación del S-TAP de HPUC mediante el instalador nativo

Procedimiento

Para eliminar el S-TAP de HPUX mediante el instalador nativo, utilice el mandato siguiente:

```
swremove @<hostname>:/var/spool/sw
```

Instalación y desinstalación de S-TAP con el instalador nativo de Solaris

Acerca de esta tarea

Procedimiento

1. Obtenga la dirección IP del servidor de base de datos en el que está instalando S-TAP. Si se utilizan IP virtuales, anótelas también (tendrá que configurarlas más adelante, cuando complete la configuración).
2. Identifique la dirección IP del recopilador que controlará esta instancia de S-TAP y a la que informará esta instancia de S-TAP.
3. Verifica la conectividad entre el servidor de bases de datos y el recopilador. En la base de datos, especifique nmap -p <puerto> <dirección_ip>. Por ejemplo, para comprobar que el puerto 16018 (el puerto que Guardium utiliza para TLS) es accesible en la dirección IP 192.168.3.104, especifique el mandato
   nmap -p 16018 192.168.3.104
   La salida típica es parecida a la siguiente:
   `Starting nmap V. 3.00 Interesting ports on g4.guardium.com (192.168.3.104): Port State Service 16018/tcp open unknown`
4. Localice el archivo del instalador nativo adecuado (archivo .pkg) en el DVD de instalación de Guardium S-TAP para su versión de Solaris
5. Especifique el mandato pkgadd para ejecutar el instalador utilizando el archivo seleccionado:

   ```
   pkgadd -d <filename>.pkg
   ```

   El instalador de shell se extrae bajo /usr/local/guardium

6. Continúe en el Paso 6 del procedimiento de instalación, ejecutando el script de instalación de shell extraído en lugar del script de instalación predeterminado para la versión del sistema operativo.

Tema principal: Instalación y desinstalación de un S-TAP de Linux, Solaris, AIX y HP-UX con un instalador nativo

Eliminación del S-TAP de Solaris mediante el instalador nativo

Procedimiento

Para eliminar la instancia de S-TAP de AIX mediante el instalador nativo:

```
pkgrm GrdTapIns
```

Desinstalación de S-TAP

Lleve a cabo este procedimiento antes de instalar una nueva versión de S-TAP si desea guardar el archivo de configuración antiguo.

Acerca de esta tarea

Si un S-TAP se ha instalado anteriormente, existe un directorio denominado: /usr/local/guardium/guard_stap.

Si ha instalado A-TAP, debe desactivarlo antes de intentar cualquier operación de actualización/instalación; consulte la descripción del mandato de desactivación de A-TAP en Desactivación de A-TAP.

Si va a eliminar una versión anterior de S-TAP que ha utilizado K-TAP, tendrá que reiniciar el servidor de base de datos. Si se ha instalado K-TAP, tendrá un archivo de dispositivo denominado: /dev/guard_ktap.

Procedimiento

1. Inicie la sesión en el sistema del servidor de base de datos utilizando la cuenta root.
2. De forma opcional, copie el archivo de configuración de S-TAP en una ubicación segura (un directorio que no sea Guardium). De forma predeterminada, el nombre de vía de acceso completo es: /usr/local/guardium/guard_stap/guard_tap.ini. Puede utilizar este archivo más adelante si tiene que volver a instalar esta versión del software o puede hacer referencia al mismo cuando configure una versión actualizada de S-TAP. No utilice nunca un archivo de configuración antiguo directamente con una versión más reciente del software; es posible que falten las propiedades más recientes y que los valores predeterminados den lugar a un comportamiento inesperado al iniciar S-TAP.
3. Ejecute el script de desinstalación. Por ejemplo, si se ha utilizado el directorio predeterminado: `[root@yourserver ~]# /usr/local/guardium/guard_stap/uninstall`
4. Si la versión anterior de S-TAP incluía K-TAP, rearranque ahora el servidor de base de datos.

a. Vuelva a ejecutar el script de desinstalación.

5. Este paso sólo se aplica a las WPAR de AIX y zonas de Solaris (se omite para todas las demás). Si va a desinstalar una versión anterior de S-TAP que incluía K-TAP, emita los siguientes mandatos desde el nodo maestro: rm -f /wpars/<server>/dev/ktap* y rm -f /wpars/<server>/dev/guard_ktap*, donde /wpars/<server> es la vía de acceso entre el nodo maestro y la WPAR.

Tema principal: Instale el cliente de S-TAP en un servidor Linux, Solaris, AIX o HP-UX

Trabajar con K-TAP

K-TAP es un módulo de kernel que está instalado en el sistema operativo. Se instala durante la instalación del S-TAP. Una vez instalado, se puede habilitar o inhabilitar utilizando un valor del archivo de configuración. Cuando está habilitado, observa el acceso a un servidor de base de datos mediante un enganche con los mecanismos

utilizados para la comunicación entre el servidor y el cliente de base de datos. Con K-TAP no es necesario cambiar la forma en que los clientes de base de datos se conectan al servidor.

En el momento de la instalación, elegirá si desea o no cargar el módulo kernel de K-TAP en el sistema operativo del servidor. Esta es la única manera de cargar dicho módulo. Si inicialmente no carga K-TAP y más adelante decide que desea utilizarlo, tendrá que eliminar S-TAP y luego volver a instalarlo.
Nota: Si K-TAP no se puede cargar correctamente durante la instalación, posiblemente debido a un problema de compatibilidad de hardware o software, P-CAP se instala como mecanismo de recopilación predeterminado.
Nota: El tráfico interno de la sesión se transfiere del KTAP antiguo al nuevo KTAP mediante una devolución de llamada. Esto significa que, para la mayoría de las bases de datos, pueden ser necesarias dos solicitudes de SQL antes de que se reanude la interceptación con el nuevo KTAP para las sesiones preexistentes. En el caso de Sybase IOCP, se necesitan tres solicitudes de SQL debido a la naturaleza de la sesión.

- El mecanismo de los K-TAP
  Al instalar un S-TAP, intenta cargar la versión correcta del K-TAP. También lee la forma en la que los K-TAP manejarán las cadenas de UID.
- Creación de un K-TAP en Linux
  Hay cientos de distribuciones de Linux disponibles, y la lista va en aumento. Esto significa que es posible que todavía no haya un K-TAP disponible para su distribución de Linux. Si el K-TAP correcto no está disponible, el proceso de instalación de S-TAP lo puede crear.
- Copia de un nuevo módulo K-TAP en otros sistemas
  Cuando cree un nuevo módulo K-TAP para un servidor de base de datos Linux, puede copiar dicho módulo en otros servidores de base de datos que ejecuten la misma distribución de Linux.

Tema principal: Instale el cliente de S-TAP en un servidor Linux, Solaris, AIX o HP-UX

El mecanismo de los K-TAP

Al instalar un S-TAP, intenta cargar la versión correcta del K-TAP. También lee la forma en la que los K-TAP manejarán las cadenas de UID.

Mecanismo de cargador de KTAP

El mecanismo del cargador de KTAP utiliza la secuencia siguiente para la instalación del S-TAP de Linux (con GIM y no GIM).

Nota: El mecanismo del cargador de KTAP continuará automáticamente con el paso siguiente si el paso anterior no se ha realizado correctamente.

1. El cargador de KTAP busca una coincidencia exacta del módulo de kernel para el nivel del sistema operativo y, si lo encuentra, lo carga.
2. Si el cargador de KTAP no encuentra una coincidencia, compila el KTAP localmente y lo carga. Esto solo puede ocurrir si el sistema tiene instalados los paquetes necesarios (gcc y kernel-devel para el kernel arrancado).
3. Si el cargador de KTAP sigue sin poder cargar el módulo de kernel correcto, y si el mecanismo FlexLoad está activo, el cargador de KTAP busca el módulo de kernel coincidente más parecido y lo carga.

   Para activar el mecanismo FlexLoad, utilice los distintivos siguientes:
   - Para una instalación de shell: --ktap_allow_module_combos
   - Para una instalación de GIM: KTAP_ALLOW_MODULE_COMBOS=Y
4. Si el cargador de KTAP no puede cargar el módulo de kernel, informa con un mensaje que indica que no se ha podido realizar la carga. Instalará el S-TAP sin el K-TAP, o fallará la instalación de S-TAP. Puede entonces solicitar un módulo coincidente para su entorno al soporte de Guardium. Se tarda alrededor de dos semanas en prepararlo.

K-TAP y las cadenas de UID

Una cadena de UID es un mecanismo que permite que S-TAP (a través de K-TAP) realizar un seguimiento de la cadena de usuarios que se crea antes de una conexión a una base de datos. Se da soporte a zonas de Solaris, a WPAR de AIX, Solaris 8/9, Solaris 11 SPARC.

Un usuario puede cambiar los nombres de usuario varias veces antes de conectarse a la base de datos; por ejemplo, ejecutando ssh informix@barbet, su - db2inst1, su -, su - oracle9 y, a continuación, ejecutando sqlplus scott/tiger@onora1. Con las cadenas de UID, Guardium puede realizar un rastreo de este proceso al proceso que lo llamó, y de nuevo hasta el usuario original.

- Para zonas de Solaris, se notifican los ID de usuario en lugar de los nombres de usuario.
- La dirección IP y el puerto del cliente se añaden a la cadena de UID.
- Postgres en Solaris 11 con zonas no recibe soporte, debido a que la configuración de zona no permite el acceso de zonas maestras a esclavas en algunos directorios.
- Zonas de Solaris y WPAR de AIX: Establezca db2bp_path en el archivo guard_tap.ini con la vía de acceso completa del archivo ejecutable db2bp, la vía de acceso completa del db2bp relevante tal como se ve desde la zona/wpar global.
- No hay cadenas de UID para la comunicación entre procesos (IPC) en Solaris 8/9.
- Las cadenas de UID no se detectan para las bases de datos Hadoop.
- El parámetro hunter_trace es necesario para las conexiones TCP/IP en los S-TAP de UNIX. Establezca hunter_trace = 1 durante la instalación para habilitar uid_chain para conexiones TCP/IP locales.
- Si el proceso que inicia la sesión sale antes de que el STAP lo pueda examinar, el mecanismo para la cadena de UID no funcionará.
- La cadena de UID no da soporte a TCP local en Linux para DB2. Además, DB2 Exit requiere una versión específica de la base de datos para dar soporte a cadenas de UID.
- Cuando se ejecuta como usuario no root, la cadena de UID no funciona para la memoria compartida de DB2 (SHM) con S-TAP.
- Guardium no registra la cadena de UID para el tráfico de red.
- Es posible que Guardium no registre la cadena de UID para sesiones muy breves ya que Guardium se basa en el ID de proceso de la aplicación para determinar la cadena de UID. Si el proceso que inicia la sesión sale antes de que el STAP lo pueda examinar, el mecanismo para la cadena de UID no funcionará.

Restricción: La cadena de UID no recibe soporte en ningún escenario que requiera A-TAP para interceptar el tráfico, entre otros:

- ATAP interceptando tráfico cifrado ASO de Oracle
- ATAP interceptando tráfico cifrado de Sysbase
- ATAP interceptando tráfico cifrado de Teradata

- Tráfico de memoria compartida de DB2 o Informix en Linux (necesita ATAP)

Depuración de registros de cadena de UID

Los registros de cadena de UID con una antigüedad superior a 2 horas se depuran cuando se ejecuta el proceso de inferencia normal. Los registros con una antigüedad superior a un día se depuran cada noche.

Nota: Consulte la información sobre lotes personalizados en el tema sobre los parámetros de KTAP.
Tema principal: Trabajar con K-TAP

Creación de un K-TAP en Linux

Hay cientos de distribuciones de Linux disponibles, y la lista va en aumento. Esto significa que es posible que todavía no haya un K-TAP disponible para su distribución de Linux. Si el K-TAP correcto no está disponible, el proceso de instalación de S-TAP lo puede crear.

Cuando se instala un S-TAP en un sistema Linux, el proceso de instalación comprueba el kernel de Linux para determinar si se ha creado un K-TAP para trabajar con ese kernel. Si se está ejecutando un kernel que no ha cargado antes el KTAP, busca un módulo coincidente y lo carga. Si el proceso de instalación no encuentra un K-TAP coincidente, intenta crear uno para que coincida con el kernel de Linux.

La mayor parte del código de K-TAP es independiente del kernel. El instalador de la versión 9.1 proporciona una nueva capa de código que habilita el código independiente del kernel para que interactúe con el kernel. Esta nueva capa se distribuye como código fuente propietario. El instalador crea el K-TAP completo compilando este código fuente propietario en el kernel de Linux. Esto genera un K-TAP específico para su distribución de Linux.

Este proceso requiere que los programas de utilidad de desarrollo de kernel, que se proporcionan con la distribución de Linux, estén presentes en el servidor de base de datos en el que se va a crear el K-TAP. El paquete de desarrollo debe coincidir exactamente con el kernel. También se necesitan el compilador gcc y la versión 3.81 (y posteriores) del programa de utilidad make.

Si tiene varios sistemas que ejecutan la misma distribución de Linux, puede crear un K-TAP en un sistema y copiarlo en los demás. Por ejemplo, puede crear un K-TAP en un sistema de prueba y luego copiarlo en uno o varios servidores de base de datos de producción después de la prueba. Si utiliza Guardium Installation Manager (GIM) para instalar el S-TAP, GIM puede copiar automáticamente el lote que contiene el nuevo K-TAP en un sistema Guardium desde el que pueda distribuirlo a otros servidores de bases de datos.

Cuando el instalador intenta crear un módulo de K-TAP, verá mensajes que emite guara-ktap-loader. Estos mensajes pueden incluir:

- Está intentando compilar
- La compilación ha finalizado
- El K-TAP se ha cargado
- No se puede intentar la compilación porque no se ha encontrado el paquete de desarrollo

Tema principal: Trabajar con K-TAP
Copia de un nuevo módulo K-TAP en otros sistemas
Cómo copiar un módulo K-TAP mediante GIM

Copia de un nuevo módulo K-TAP en otros sistemas

Cuando cree un nuevo módulo K-TAP para un servidor de base de datos Linux, puede copiar dicho módulo en otros servidores de base de datos que ejecuten la misma distribución de Linux.

Antes de empezar

Siga este procedimiento después de crear y probar un módulo K-TAP en un servidor de base de datos Linux.

Acerca de esta tarea

Si utiliza Guardium Installation Manager (GIM) para gestionar agentes en los servidores de base de datos, utilice GIM para copiar el módulo. Consulte el enlace siguiente para ver el procedimiento a seguir.

Procedimiento

1. Inicie una sesión en el servidor de base de datos con el K-TAP probado.
2. Vaya al directorio /usr/local/guardium/guard_stap/ktap/current/ y ejecute ./guard_ktap_append_modules para añadir los módulos creados localmente a modules.tgz.
3. Copie el archivo actualizado de modules.tgz en el servidor de destino.
4. Inicie una sesión en el servidor de destino y vaya al directorio /usr/local/guardium/guard_stap/ktap/current/.
5. Ejecute el cargador de K-TAP con el parámetro retry y la vía de acceso completa al archivo modules.tgz actualizado. Por ejemplo:

```
guard_ktap_loader retry /tmp/modules-9.0.0_r55927_v90_1.tgz
```

6. Reinicie el S-TAP para conectarlo al nuevo módulo K-TAP.

Resultados

El módulo K-TAP personalizado está listo para utilizarse en el sistema de destino. Repita este procedimiento para cada sistema Linux en el que desee desplegar el módulo K-TAP.
Tema principal: Trabajar con K-TAP
Cómo copiar un módulo K-TAP mediante GIM
Parámetros de K-TAP

Obtención de información de Java o Perl

Es posible que tenga que comprobar la versión de Java o Perl que se está utilizando en el servidor de datos.

Obtención de información de Java

Cuando se instala CAS (Configuration Auditing System) en un sistema UNIX, hay dos requisitos:

- Debe localizar el directorio JAVA_HOME. Se le solicitará su ubicación durante la instalación de CAS.
- Debe verificar que tiene instalada una versión soportada de Java™ (consulte la tabla siguiente). Si no tiene instalada una versión soportada, debe instalarla antes de instalar CAS.

Requisitos de versión de CAS Java

Tipo de SO	Versión de Java
HP-UX	1.5 o posterior
Todos los demás	1.4.2 o posterior

Nota: Para utilizar CAS sobre SSL en un entorno compatible con FIPS, debe instalar IBM Java en el servidor en el que se ejecuta el agente de CAS.

Localice el directorio JAVA_HOME

Realice primero este procedimiento y, después de localizar el directorio JAVA_HOME, realice el siguiente procedimiento para comprobar la versión de Java.

El directorio JAVA_HOME contiene el mandato Java. Por ejemplo:

- Si el mandato java es /usr/local/j2sdk1.4.2_03/bin/java
- el directorio JAVA_HOME es /usr/local/j2sdk1.4.2_03

Utilice una de las técnicas siguientes para localizar el directorio del mandato java.

1. Escriba el mandato which java. Por ejemplo:

```
[root@yourserver ~]# which java
/usr/local/j2sdk1.4.2_03/bin/java
```

2. Si el mandato which java devuelve un enlace simbólico, utilice el mandato ls -ld <symbolic_link> para determinar el nombre del directorio real de Java.
3. Si el mandato which java devuelve un mensaje que indica que no se ha encontrado el mandato, es posible que Java esté instalado pero no esté incluido en la variable PATH. En este caso, utilice el mandato find para localizar el directorio Java; por ejemplo:

```
[root@yourserver ~]# find . -name java

./usr/bin/
```

Determine la versión de Java

1. Desde el directorio java, ejecute el mandato java -version para comprobar el número de versión. Por ejemplo:

```
[root@yourserver ~]# /usr/local/j2sdk1.4.2_03/bin/java -version
java version "1.4.2_03"
Java(TM) 2 Runtime Environment, Standard Edition (build 1.4.2_03-b02)
Java HotSpot(TM) Client VM (build 1.4.2_03-b02, mixed mode)
```

2. Anote la versión de Java que se devuelve. No se le solicitará esta información, pero en el caso de que se produzca un problema más tarde, podrá eliminar la posibilidad de una versión de Java no soportada.

Obtención de información de Perl

Este requisito de Perl sólo se aplica a la combinación siguiente:

- Unix S-TAP
- El mecanismo TEE seleccionado para supervisar el tráfico local
- El proceso Hunter se utiliza para detectar y opcionalmente interrumpir procesos que pasan por alto el puerto de escucha Tee

En esta situación, debe tener:

- Versión 5.8.0 o posterior de Perl
- Perl debe estar instalado en el directorio /usr/bin

Para verificar que tiene instalada la versión, utilice el mandato siguiente:

```
/usr/bin/perl -v
```

Si Perl no está instalado, está instalado en otro directorio o tiene instalada una versión anterior, debe instalar la versión 5.8.0 o posterior de Perl en el directorio /usr/bin antes de instalar S-TAP.

Tema principal: Instale el cliente de S-TAP en un servidor Linux, Solaris, AIX o HP-UX

Cuándo reiniciar o rearrancar la base de datos después de la instalación o actualización de S-TAP

En este tema se detallen los casos, después de la instalación de S-TAP, en que se debe reiniciar o se debe rearrancar la instancia de la base de datos o el servidor de base de datos. Se cubren los S-TAP tanto de Windows como de UNIX/Linux. Se cubren las versiones v9.0/9.1/9.5 y v10.0/10.1. Los requisitos de reinicio/rearranque son los mismos para las implementaciones de GIM y no de GIM.

Lo que se debe reiniciar después de una nueva instalación de un S-TAP de UNIX/Linux

Para ver el tráfico completo, ciertas bases de datos se deben reiniciar después de una instalación de S-TAP.

Tabla 1. Reinicio de base de datos después de la instalación de S-TAP

SO/Base de datos	Oracle		DB2		Sybase		MS-SQL		Informix	
	TPC/IPC	SHM	TPC/IPC	SHM	TPC/IPC	SHM	TPC/IPC	SHM	TPC/IPC	SHM
RedHat	NR	NR	NR	REQ-Exit	NR	NR	NR	NR	NR	REQ-Exit
SuSE	NR	NR	NR	REQ-Exit	NR	NR	NR	NR	NR	REQ-Exit
AIX	REQ*	NR	REQ	NR	REQ	NR	NA	NR	REQ	NR
Solaris	NR	NR	NR	NR	NR	NR	NR	NR	NR	NR
HP-UX	NR	NR	NR	NR	NR	NR	NR	NR	NR	NR
Windows	NR		NR		NR		NR		NR	

SHM - Memoria compartida

NR = No es necesario reiniciar/rearrancar (basado en el uso de un mecanismo de actualización dinámica y haciendo referencia a un enlace de actualización dinámica si dispone de uno)

REQ = Es necesario reiniciar

REQ-W = Solo es necesario reiniciar la instancia de base de datos para una instalación nueva de S-TAP de Windows v8 y v9 (no es necesario reiniciar el servidor de base de datos), no es necesario reiniciar el servidor de base de datos ni la instancia de base de datos para una actualización dinámica. No es necesario reiniciar para una instalación nueva de S-TAP de Windows v10.x.

REQ * = es necesario reiniciar la base de datos y la escucha

REQ-Exit = En este caso, se necesita un A-TAP o controlador de Exit para capturar el tráfico de la memoria compartida. Es necesario reiniciar la base de datos para poder activar el proceso.

NA = no se aplica

Nota: Base de datos MySQL con base de datos RedHat - NR
Nota: Es necesario reiniciar la instancia de base de datos en los casos en los que se utilice la agrupación de conexiones. (Es necesario reiniciar la escucha de BD en un entorno de servidor de aplicaciones porque todas las sesiones se tienen que desconectar y luego volver a conectar).
Nota: (S-TAP de UNIX/Linux V10.0) - Nada cambia en lo referencia a cuándo hay que reiniciar, pero en la v10. Guardium ya no da soporte al "script guard-stap-update". En su lugar, el instalador de shell proporcionado tiene incorporada la lógica de actualización, por lo tanto solo hay que ejecutar el nuevo instalador.

Lo que se debe reiniciar después de una actualización dinámica de un S-TAP de UNIX/Linux

No es necesario reiniciar nada para las actualizaciones dinámicas que no incluyen ATAP.

S-TAP de Windows

Hay que distinguir entre una instalación de Windows nueva y una actualización dinámica.

Todas las instancias de base de datos se deben reiniciar (no rearrancar) cuando se realiza una instalación desde cero (instalación nueva). Consulte la excepción a la información cuando se utiliza el controlador de WFP V10.0. No es necesario reiniciar la instancia de la base de datos tras una actualización dinámica.

No es necesario rearrancar el servidor Windows, a menos que se actualice desde V7.0. La razón es que la actualización desde V7.0 requiere una desinstalación completa del software S-TAP. Sin embargo, si se actualizan los archivos del controlador de proxy, es necesario rearracar del sistema. Ejemplos de archivos de controlador proxy: NmpProxy.sys. Nota: Para cada release, compruebe el documento del release para ver si se actualizan los controladores de proxy.

Es necesario rearrancar si se actualiza desde Guardium V7.0. Esto se aplica a todos los métodos de instalación/actualización: GIM, Interactivo o Por lotes.

El STAP de Windows V10.0 utiliza un nuevo controlador de WFP (plataforma de filtrado de Windows). Este controlador de WFP sustituye al controlador TCP basado en TDI (Interfaz de controlador de transporte). Wfpmonitor es el nuevo controlador TCP de S-TAP, que sustituye a lhmonproxy y lhmon. WFP ofrece las siguientes ventajas:

- Se puede actualizar sin necesidad de rearrancar.
- No es necesario reiniciar las instancias de base de datos para recoger el tráfico TCP después de una instalación nueva.
- Ahora todos los controladores proporcionan un recurso de registro (cíclico). Los archivos de registro se encuentran en /logs. Esto mejora la capacidad de soporte, ya que los errores/avisos del controlador no estaban visibles.

S-TAP de UNIX/Linux

Sin rearranque

S-TAP/KTAP se puede actualizar sin un rearranque cuando se utiliza el programa de utilidad "guard-stap-update". Este programa de utilidad se puede utilizar desde la versión V8.0 y siguientes. (Para los S-TAP de UNIX-Linux v10.0, consulte la nota anterior sobre que Guardium ya no da soporte al programa de utilidad "guard-stap-update").

Si el sistema se "actualiza" desde una versión que no es de GIM a la misma versión de GIM, no es necesario rearrancar el sistema.

Si se actualiza un S-TAP no GIM con GIM BUNDLE-STAP, con el mismo número de revisión que se está ejecutando actualmente, no es necesario rearrancar.

La actualización de GIM de lote (además de la actualización de S-TAP de lote) SOLO es necesaria en los siguientes casos de actualización:

- Se pasa de V8 a V9.
- Si tiene instalado un S-TAP de lote V9 con un parche ANTERIOR a V9.0 parche 100 o un número de compilación ANTERIOR a 9.0.0_r57263.
- Todos los demás casos de actualización NO necesitan la actualización de GIM de lote.

Rearranque necesario

Es necesario rearrancar el servidor de base de datos si se actualiza desde Guardium V7.0.

Actualización del S-TAP durante el siguiente rearranque con el programa de utilidad Guardium Upgrader. El uso de este programa de utilidad requiere un rearranque.

Si va a eliminar una versión anterior de S-TAP que utilizaba KTAP, tendrá que rearrancar el servidor de base de datos.

Cuando actualice S-TAP mediante GIM:

- Si se especifica KTAP_LIVE_UPDATE=Y, no es necesario rearrancar.
- Si se especifica KTAP_LIVE_UPDATE=N, es necesario rearrancar.

Si se actualiza un S-TAP no GIM con GIM BUNDLE-STAP, con un número de revisión distinto del que se está ejecutando actualmente, es necesario rearrancar.

Para volver a instalar un S-TAP con KTAP utilizando el mismo número de revisión, es necesario desinstalar y rearrancar.

Después de la instalación de ATAP de UNIX en un entorno de clúster de Oracle, se deben reiniciar las instancias, así como todos los procesos entre clústeres.

Requisitos de reinicio/carga/instrumentación/activación para ATAP

ATAP o S-TAP o KTAP no se rearrancan.

S-TAP se detiene/inicia/reinicia. KTAP se carga/descarga. ATAP se instrumenta/activa/desactiva/desinstrumenta.

Las instancias de base de datos que necesitan ATAP se deben detener antes de la instrumentación (si es necesaria) y la activación.

La desinstrumentación o desactivación de ATAP también requiere que se detengan las instancias de base de datos.

Debe se debe desactivar (y desinstrumentar, si procede), antes de cualquier actualización de la base de datos, por ejemplo cuando se aplica un Fixpack.

Por último, ATAP se debe desactivar y desinstrumentar antes de cualquier actualización de S-TAP (no es necesario para las actualizaciones de lote de GIM).

Tema principal: Instalación de S-TAP

Equilibrio de carga empresarial

El equilibrador de carga empresarial asigna de forma dinámica unidades gestionadas a agentes de S-TAP en función de la carga y la disponibilidad del sistema.

Visión general

El equilibrio de carga asigna automáticamente unidades gestionadas a agentes de S-TAP cuando se instalan nuevos S-TAPs y durante la sustitución por anomalía cuando una unidad gestionada no está disponible. La aplicación de equilibrio de carga también reequilibra de forma dinámica las unidades gestionadas u ocupadas mediante la reubicación de agentes de S-TAP a unidades gestionadas menos cargadas.

La aplicación de equilibrio de carga empresarial automatiza varias tareas:

- El equilibrio de carga elimina la necesidad de evaluar manualmente la carga de las unidades gestionadas antes de asignar esas unidades gestionadas a un agente de S-TAP.
- El equilibrio de carga elimina la necesidad de definir unidades gestionadas de sustitución por anomalía como parte de la configuración de S-TAP posterior a la instalación ya que el equilibrador de carga gestiona de forma dinámica los escenarios de sustitución por anomalía.
- El equilibrio de carga elimina la necesidad de reubicar manualmente los agentes de S-TAP de las unidades gestionadas cargadas en unidades gestionadas menos cargadas.

Importante: Cuando se utiliza la aplicación de equilibrio de carga empresarial, el sistema Guardium toma el control sobre la asignación de unidades gestionadas a agentes de S-TAP. Este es un proceso automatizado y dinámico: verá una asociación de cambio de S-TAPs basada en la carga relativa de las unidades de trabajo disponibles. Utilice el informe Sucesos del equilibrador de carga para revisar toda la actividad de equilibrio de carga.
Nota: Cuando se configura el S-TAP para que utilice el equilibrio de carga empresarial, no se puede utilizar el equilibrio de carga basado en F5.

Requisitos previos

El equilibrador de carga empresarial se ejecuta en un gestor central o en una unidad gestionada, escucha en el puerto 8443 y utiliza la seguridad de la capa de transporte (TLS). No es necesario ningún nuevo cortafuegos ni ninguna configuración del sistema adicional. Si se configura el equilibrador de carga empresarial para que se ejecute en una unidad gestionada, los S-TAP deben tener el nivel V10.1 o posterior.

El equilibrio de carga está habilitado de forma predeterminada en los sistemas Guardium. Para obtener información sobre cómo habilitar S-TAPs para que participe en el equilibrio de carga, consulte Configuración de instalaciones de S-TAP para el equilibrio de carga empresarial.

Cómo funciona

La aplicación de equilibrio de carga empresarial funciona recopilando y manteniendo información de carga actualizada de todas sus unidades gestionadas.

Utiliza la información de carga de las unidades gestionadas para crear un mapa de carga. Este mapa de carga proporciona los datos que dirigen las actividades de equilibrio de carga y de asignación de unidad gestionada. Utilice el mandato de GuardAPI grdapi get_load_balancer_load_map para ver el mapa de carga actual en cualquier momento.

La información de carga sólo se recopila de las unidades gestionadas que están en línea y configuradas con el parámetro LOAD_BALANCER_ENABLED=1. Al establecer LOAD_BALANCER_ENABLED=0 se inhabilita el equilibrio de carga y se impide que esa unidad gestionada se asigne dinámicamente a los agentes de S-TAP durante las actividades de equilibrio de carga.

Los errores de recopilación de carga procedentes de unidades gestionadas específicas se registran en el informe Sucesos del equilibrador de carga, pero no interfieren con los procesos de recopilación de carga y equilibrio de carga. Sin embargo, si no se puede recopilar información de una unidad gestionada, se excluye esa unidad de los procesos de equilibrio de carga.

- Utilización del equilibrio de carga empresarial
  Siga esta secuencia de tareas para empezar a utilizar la función de equilibrio de carga empresarial.

- Parámetros de configuración del equilibrio de carga empresarial
  Esta información de consulta contiene descripciones detalladas de los parámetros de configuración del equilibrador de carga. En un Gestor central (CM), acceda desde Gestionar > Gestión central > Equilibrio de carga empresarial > Propiedades del equilibrio de carga empresarial. En una unidad gestionada (MU), acceda desde Configuración > Gestión central > Registro y equilibrio de carga.

Tema principal: S-TAPs y otros agentes

Utilización del equilibrio de carga empresarial

Siga esta secuencia de tareas para empezar a utilizar la función de equilibrio de carga empresarial.

1. Configuración de instalaciones de S-TAP para el equilibrio de carga empresarial
   Aprenda a utilizar el equilibrio de carga empresarial al instalar un agente de S-TAP.
2. Asociación de S-TAP con unidades gestionadas para el equilibrio de carga
   Aprenda a utilizar el equilibrio de carga empresarial mediante la creación y asociación de grupos de S-TAP con grupos de unidades gestionadas.
3. Visualización del mapa de carga de equilibrio de carga empresarial
   Aprenda a ver el mapa de carga del equilibrador de carga empresarial actual.
4. Visualización de un informe de actividad de equilibrio de carga empresarial
   Vea un informe de actividades y sucesos de equilibrio de carga.

Tema principal: Equilibrio de carga empresarial

Configuración de instalaciones de S-TAP para el equilibrio de carga empresarial

Aprenda a utilizar el equilibrio de carga empresarial al instalar un agente de S-TAP.

Procedimiento

Especifique los parámetros de equilibrio de carga empresarial durante la instalación de S-TAP. Los mismos parámetros están disponibles si se utilizan instaladores de línea de mandatos o el instalador de GIM.
Nota: Cuando se instalan los S-TAP mediante la línea de mandatos y las opciones del equilibrador de carga especifican una dirección IP distinta de la dirección predeterminada, es posible que el equilibrador de carga asigne de forma incorrecta las unidades gestionadas. Esto sucede cuando la dirección IP de cliente predeterminada se envía al equilibrador de carga antes de que se proporcione la dirección no predeterminada durante la instalación S-TAP.
Nota: Para los parámetros enumerados en la tabla siguiente utilice -- (dos guiones) antes del parámetro para UNIX/Linux y un único guión para Windows. Por ejemplo, UNIX/Linux: --load-balancer-ip. Windows: -load-balancer-ip

Tabla 1. Parámetros de instalación de S-TAP para el equilibrio de carga empresarial

Parámetro para instaladores interactivos	Parámetro para instaladores de GIM	Descripción
--load-balancer-ip load_balancer_ip	STAP_LOAD_BALANCER_IP	Obligatorio. Esta opción especifica la dirección IP del gestor central o de la unidad gestionada que debe utilizar este S-TAP para el equilibrio de carga. Notas: • Si utiliza el equilibrio de carga empresarial cuando participate_in_load_balancing=0 y num_mus > 1, los datos de sustitución por anomalía no se enviarán al sistema secundario. En su lugar, los datos de sustitución por anomalía se enviarán al sistema asignado por el equilibrador de carga para sustituir el servidor anómalo. Esto solo se aplica si el gestor central se está ejecutando y el equilibrador de carga empresarial está activo. Si el equilibrador de carga no está disponible, el tráfico se redireccionará al sqlguard_ip secundario. • Los parámetros de S-TAP de Windows no se pueden cambiar mediante el instalador interactivo durante una actualización. Utilice la interfaz de usuario de Guardium después de la actualización para cambiar los parámetros de S-TAP de Windows. • Si se configura el equilibrador de carga empresarial para que se ejecute en una unidad gestionada, el S-TAP debe tener el nivel V10.1 o posterior.
--lb-app-group app_group	STAP_INITIAL_BALANCER_TAP_GROUP	Opcional. Esta opción especifica el grupo de S-TAP al que pertenecerá este S-TAP. Atención: Los nombres de grupo con espacios o caracteres especiales no reciben soporte.
--lb-mu-group mu_group	STAP_INITIAL_BALANCER_MU_GROUP	Opcional. Esta opción especifica el grupo de unidades gestionadas al que se asociará el grupo de aplicaciones. También se debe especificar un grupo de aplicaciones para utilizar este parámetro. Notas: Los nombres de grupo con espacios o caracteres especiales no reciben soporte. Este parámetro solo se puede especificar una vez, durante la instalación inicial. Debe existir un grupo de MU en el gestor central para que se pueda utilizar durante la instalación de S-TAP. Atención: Los nombres de grupo con espacios o caracteres especiales no reciben soporte.
--lb-num-mus number_of_mus	STAP_LOAD_BALANCER_NUM_MUS	Opcional. Esta opción especifica el número de unidades gestionadas que debe asignar el equilibrador de carga para este S-TAP.

Tema principal: Utilización del equilibrio de carga empresarial
Tema siguiente: Asociación de S-TAP con unidades gestionadas para el equilibrio de carga

Asociación de S-TAP con unidades gestionadas para el equilibrio de carga

Aprenda a utilizar el equilibrio de carga empresarial mediante la creación y asociación de grupos de S-TAP con grupos de unidades gestionadas.

Acerca de esta tarea

El equilibrio de carga crea asociaciones entre grupos de S-TAP y grupos de unidades gestionadas de forma que los S-TAPs de un grupo se puedan reasignar a la unidad gestionada con mayor disponibilidad dentro de un grupo. Esta tarea presenta el proceso de establecimiento de asociaciones entre los grupos de S-TAP y los grupos de unidades gestionadas para conseguir el equilibrio de carga empresarial.

Procedimiento

1. En un gestor central, vaya a Gestionar > Gestión central > Equilibrador de carga empresarial > Asociar S-TAP y unidades gestionadas.
2. Si aún no se a creado un grupo de S-TAP o si se necesita uno nuevo, cree un grupo de S-TAP.
   a. Pulse el icono para abrir el diálogo Crear nuevo grupo de S-TAP.
   b. Especifique un nombre en el campo Nombre de grupo. Por ejemplo, `North_American_S-TAPs`.
      Recomendación: Para garantizar la compatibilidad con otros componentes de Guardium, no utilice espacios ni caracteres especiales en los nombres de grupo.
   c. Añada miembros al grupo seleccionando entre nombres de host existentes o añadiendo miembros nuevos mediante el campo Miembro de grupo. Los S-TAPs indicados con un icono se incluyen con el nuevo grupo de S-TAP.
   d. Pulse Crear nuevo grupo para crear el grupo de S-TAP.
3. Asocie el grupo de S-TAP con un grupo de unidades gestionadas.
   a. Seleccione el grupo de S-TAP que desea asociar. Por ejemplo, `North_American_S-TAPS`.
   b. Pulse Asociar unidades gestionadas para abrir el diálogo Asociar grupo de unidades gestionadas.
   c. Si es necesario, cree un nuevo grupo de unidades gestionadas.
      i. Vaya a Gestionar > Gestión central > Grupos de unidades gestionadas.
      ii. Pulse el icono para abrir el diálogo Crear nuevo grupo de unidades gestionadas.
      iii. Especifique un nombre en el campo Nombre de grupo. Por ejemplo, `North_American_MU`.
      Recomendación: Para garantizar la compatibilidad con otros componentes de Guardium, no utilice espacios ni caracteres especiales en los nombres de grupo.
      iv. Añada miembros al grupo seleccionando las Direcciones IP de unidad gestionada existentes.
      v. Pulse Crear nuevo grupo para crear el nuevo grupo de unidades gestionadas.
   d. Seleccione el grupo o grupos de unidades gestionadas que se deben asociar al grupo de S-TAP. Por ejemplo, `North_American_MU`.
   e. Pulse Aplicar.
4. Pulse Guardar para completar la asociación entre un grupo de S-TAP y un grupo de unidades gestionadas.
5. (Opcional) Asocie el grupo de S-TAP con un grupo de sustitución por anomalía de unidades gestionadas.
   a. Seleccione el grupo de S-TAP que desea asociar, que ya está asociado a un grupo de unidades gestionadas. Por ejemplo, North_American_S-TAPS.
   b. Pulse Asociar grupos de sustitución por anomalía para abrir el diálogo Asociar grupo de sustitución por anomalía.
   c. Si es necesario, cree un nuevo grupo de unidades gestionadas tal como que se ha descrito anteriormente. Los grupos de unidades gestionadas normales y los grupos de sustitución por anomalía son los mismos hasta que se especifican durante la asociación con el grupo S-TAP.
   d. Seleccione el grupo o grupos de unidades gestionadas que se deben asociar al grupo de S-TAP. Por ejemplo, North_American_MUs_failover.
   e. Pulse Aplicar.
6. Pulse Guardar para completar la asociación entre un grupo de S-TAP y un grupo de unidades gestionadas.

Tema principal: Utilización del equilibrio de carga empresarial
Tema anterior: Configuración de instalaciones de S-TAP para el equilibrio de carga empresarial
Tema siguiente: Visualización del mapa de carga de equilibrio de carga empresarial

Visualización del mapa de carga de equilibrio de carga empresarial

Aprenda a ver el mapa de carga del equilibrador de carga empresarial actual.

Acerca de esta tarea

La aplicación de equilibrio de carga empresarial utiliza la información de carga de las unidades gestionadas para crear un mapa de carga. Este mapa de carga proporciona los datos que dirigen las actividades de equilibrio de carga y de asignación de unidad gestionada.

Procedimiento

1. Para ver el mapa de carga actual como un informe en la interfaz de usuario de Guardium, vaya a Gestionar > Informes > Utilización de la unidad > Equilibrador de carga.
2. También se puede ver el mapa de carga actual mediante la API de Guardium. Emita el siguiente mandato de GuardAPI: grdapi get_load_balancer_load_map.

   El mapa de carga debe ser similar al del ejemplo siguiente:

```
ID=0

************ LOAD MAP *************

****************  LOADED MU LIST ************************

****************  VACANT MU LIST ************************
  {
   MU=myguard_01.domain.com
   MU_QUEUE_SIZE(MB)=25.0
```

```
    MU_TIMES_REBALANED=0
    MU_EFFECTIVE_MAX_USED_QUEUE(%)=0.0
    MU_MAX_LOAD_CONTIB_BY_STAP(MB)=0.0
    MU_ADJUSTED_STAP_CONTRIB_IN_MB=0.0
    MU_BASE_MAX_USED_QUEUE_IN_MB=0.0
    IS_REBALANCABLE=true
    INSTALLED_POLICIES=log full details|
    APPLIANCE_RESOURCE_INFO={NUM_PROCESSORS=4,CPU_SPEED=2800,CPU_CACHE=25600,CPU_CORES=4,
       CACHE_READ_RATE=7870,HARD_DRIVE_READ_RATE=186,MEMORY_SIZE=24607}
    STAP_LIST=
        {
        STAP_IP=01_gct1.domain.com, STAP_HOST=01_gct1.domain.com, CONNECTED_TO_MU=gct1.domain.com,
           PARTICIPATES_IN_LOAD_BALANCING=false, MAX_STAP_CONTIBUTION_TO_LOAD_IN_MB=0.0,
           AVG_STAP_CONTIBUTION_TO_LOAD_IN_MB=0.0
        }
        {
        STAP_IP=02_gct1.domain.com, STAP_HOST=02_gct1.domain.com, CONNECTED_TO_MU=gct1.domain.com,
           PARTICIPATES_IN_LOAD_BALANCING=false, MAX_STAP_CONTIBUTION_TO_LOAD_IN_MB=0.0,
           AVG_STAP_CONTIBUTION_TO_LOAD_IN_MB=0.0
        }
        {
        STAP_IP=03_gct1.domain.com, STAP_HOST=03_gct1.domain.com, CONNECTED_TO_MU=gct1.domain.com,
           PARTICIPATES_IN_LOAD_BALANCING=false, MAX_STAP_CONTIBUTION_TO_LOAD_IN_MB=0.0,
           AVG_STAP_CONTIBUTION_TO_LOAD_IN_MB=0.0
        }
  }

**********  STAP -> MUS ALLOCATION TABLE **********
03_gct1.domain.com ----> gct1.domain.com
02_gct1.domain.com ----> gct1.domain.com
01_gct1.domain.com ----> gct1.domain.com
ok
```

Tema principal: Utilización del equilibrio de carga empresarial
Tema anterior: Asociación de S-TAP con unidades gestionadas para el equilibrio de carga
Tema siguiente: Visualización de un informe de actividad de equilibrio de carga empresarial

Visualización de un informe de actividad de equilibrio de carga empresarial

Vea un informe de actividades y sucesos de equilibrio de carga.

Acerca de esta tarea

El informe Sucesos del equilibrador de carga empresarial muestra todos los sucesos y actividades de equilibrio de carga, incluidas las asociaciones correctas entre agentes y unidades gestionadas de S-TAP, los cambios en la carga de la unidad gestionada y las asociaciones anómalas.

Procedimiento

Para ver el informe, vaya a Gestionar > Informes > Supervisión de actividad > Sucesos del equilibrador de carga empresarial.

Tema principal: Utilización del equilibrio de carga empresarial
Tema anterior: Visualización del mapa de carga de equilibrio de carga empresarial

Parámetros de configuración del equilibrio de carga empresarial

Esta información de consulta contiene descripciones detalladas de los parámetros de configuración del equilibrador de carga. En un Gestor central (CM), acceda desde Gestionar > Gestión central > Equilibrio de carga empresarial > Propiedades del equilibrio de carga empresarial. En una unidad gestionada (MU), acceda desde Configuración > Gestión central > Registro y equilibrio de carga.

Parámetro	Valor predeterminado (valores válidos)	Descripción
STATIC_LOAD_COLLECTION_INTERVAL	720 (≥10)	Intervalo de recopilación de carga de unidad gestionada estática (en minutos). Si ENABLE_DYNAMIC_LOAD_COLLECTION se establece en 0, el equilibrador de carga recopila la carga de todas las unidades gestionadas en el intervalo especificado en STATIC_LOAD_COLLECTION_INTERVAL.
LOAD_BALANCER_ENABLED	1 (0 ó 1)	Controla la característica del equilibrador de carga. • 0 inhabilita la característica • 1 habilita la característica Si no inhabilitado en la unidad gestionada, el equilibrador de carga (que se ejecuta en el gestor central) no recopila información de carga de esa unidad gestionada. Los S-TAPs conectados a esa unidad gestionada no participan en el equilibrio de carga. En el CM, cuando se habilita este parámetro (después de que se haya inhabilitado) se activa una recopilación de carga completa inmediata desde todas las unidades gestionadas habilitadas para el equilibrio de carga.
ENABLE_DYNAMIC_LOAD_COLLECTION	1 (0 ó 1)	Controla el método de recopilación de carga. • 0 inhabilita el intervalo de recopilación de carga dinámica (utiliza STATIC_LOAD_COLLECTION_INTERVAL como intervalo de recopilación) • 1 habilita el intervalo de recopilación de carga dinámica

		Cuando este parámetro está habilitado (establecido en `1`), el intervalo de recopilación es proporcional al número de unidades gestionadas (1 hora por cada 10 unidades gestionadas conectadas). Los cambios en este parámetro activan un nuevo cálculo inmediato del tiempo de recopilación de la carga completa.
USE_APPLIANCE_HW_PROFILE_FACTOR	1 (0 ó 1)	El equilibrador de carga puede utilizar indicadores de perfil de hardware de las unidades (especificados mediante el parámetro APPLIANCE_HW_PROFILE_INDICATORS) al evaluar las unidades gestionadas libres para la reubicación de S-TAPs. • `0` pasa por alto los indicadores del perfil de hardware • `1` utiliza indicadores del perfil de hardware de unidades gestionadas
MAX_RELOCATIONS_BETWEEN_FULL_LOAD_COLLECTIONS	3 (≥-1)	Define el número máximo de reubicaciones de S-TAP (entre unidades gestionadas) permitido después de una recopilación de carga completa. Los valores negativos significan que se permite un número ilimitado de reubicaciones.
ALLOW_POLICY_MISMATCH_BETWEEN_APPLIANCES	1 (0 ó 1)	El equilibrador de carga puede tener en cuenta las políticas instaladas de las unidades gestionadas. • `0` no permite la reubicación de S-TAP cuando hay una discrepancia de política entre las unidades gestionadas de origen y de destino. • `1` permite la reubicación de S-TAPs incluso si hay una discrepancia de política entre las unidades gestionadas de origen y de destino. •
TIME_TO_IGNORE_STAP_CONNECTION_RELATED_LOAD	10 (≥5)	Cuando se recopilan estadísticas de carga para S-TAPs de cada unidad gestionada, se desea evitar la inclusión de los datos que representan la conexión inicial de S-TAP con la unidad gestionada. Estos datos pueden indicar picos de tráfico que crean un falso positivo para el equilibrador de carga. El parámetro TIME_TO_IGNORE_STAP_CONNECTION_RELATED_LOAD indica al equilibrador de carga que pase por alto la carga de S-TAP durante el número de minutos especificado después de que el S-TAP se haya conectado a la unidad gestionada.
ENABLE_RELOCATION	1 (0 ó 1)	La reubicación de recursos (reequilibrio) es un proceso que el equilibrador de carga ejecuta después de una recopilación de carga completa. La reubicación aquí significa transferir S-TAPs de unidades gestionadas cargadas a unidades gestionadas libres. • `0` no permite la reubicación de S-TAPs en unidades gestionadas libres • `1` permite reubicar S-TAPs en unidades gestionadas libres
LOADED_SNIFFER_QUEUE_USAGE_THRESHOLD	0.6 (0.1 a 1 en incrementos de 0.1)	Se considera que una unidad gestionada está cargada si su sniffer tiene al menos una cola cuyo tamaño alcanza LOADED_SNIFFER_QUEUE_ USAGE_THRESHOLD. El tamaño de la cola de sniffer se define mediante el parámetro ADMINCONSOLE_PARAMETER_DEFAULT_QUEUE_SIZE. Este parámetro no se debe cambiar en circunstancias normales.
DEFAULT_STAP_MAX_QUEUE_USAGE	0.15 (0.10 a 1 en incrementos de 0.10)	Cuando un S-TAP se asigna inicialmente a una unidad gestionada, el equilibrador de carga no tiene información sobre el mismo. El valor de este parámetro define la cola máxima utilizada del sniffer temporal hasta que se recopila la carga real desde la unidad gestionada (después del intervalo definido por el parámetro TIME_TO_IGNORE_STAP_CONNECTION_RELATED_LOAD). Este parámetro no se debe cambiar en circunstancias normales.
DEFAULT_STAP_MAX_CONTRIBUTION_TO_MAX_QUEUE_USAGE	0.1 (0.1 a 1 en incrementos de 0.1)	Cuando un S-TAP se asigna inicialmente a una unidad gestionada, el equilibrador de carga no tiene información sobre el mismo. El valor de este parámetro define la contribución temporal máxima de carga de S-TAP a la cola máxima temporal utilizada hasta que se recopila la carga real desde la unidad gestionada (después del intervalo definido por el parámetro TIME_TO_IGNORE_STAP_CONNECTION_RELATED_LOAD). Este parámetro no se debe cambiar en circunstancias normales.
REBALANCE_IF_MU_CLASSIFIED_AS_LOADED_N_TIMES_IN_M_HOURS	1:168 (≥0 : ≥0)	Las unidades gestionadas cargadas solo se pueden volver a equilibrar si se han clasificado como si fueran un número especificado de instancias durante un periodo de horas especificado. Por ejemplo, el valor `1:168` requiere que una unidad gestionada se clasifique como cargada al menos `1` vez durante un periodo de `168` horas.
APPLIANCE_HW_PROFILE_INDICATORS	NUM_PROCESSORS: CPU_SPEED: CPU_CACHE: CPU_CORES: MEMORY_SIZE (Nombre de columnas de la tabla *APPLIANCE_RESOURCE_INFO*)	El equilibrador de carga puede tener en cuenta las indicadores del perfil de hardware de la unidad. El equilibrador de carga utiliza una lista de indicadores delimitada por dos puntos (nombres de columna de la tabla *APPLIANCE_RESOURCE_INFO*) para evaluar el perfil de hardware. Este parámetro no se debe cambiar en circunstancias normales.
MAX_CONCURRENT_LOAD_COLLECTIONS	10 (≥1)	El número máximo de procesos de recopilación de carga simultáneos que ejecuta el equilibrador de carga en un determinado punto en el tiempo. Es decir, el número de conexiones de SQL remotas, no permanentes y permanentes entre el gestor ventral y la unidad gestionada.
MAX_RELOCATIONS_PER_MU_BETWEEN_FULL_LOAD_COLLECTIONS	3 (≥-1)	El número máximo de reubicaciones de S-TAP permitidas desde una unidad gestionada específica. Los valores negativos permiten un número ilimitado de reubicaciones.
ENABLE_FAILOVER_GROUPS_REBALANCE	0 (0 ó 1)	Controla la reubicación automática de S-TAP desde el grupo de sustitución por anomalía en el grupo de MU principal una vez que una MU está disponible de nuevo en el grupo de MU principal.

		0 no permite la reubicación automática de S-TAP de nuevo en el grupo principal de MU 1 permite la reubicación automática de S-TAP de nuevo en el grupo principal de MU

Tema principal: Equilibrio de carga empresarial

Tráfico de base de datos autenticado mediante Kerberos

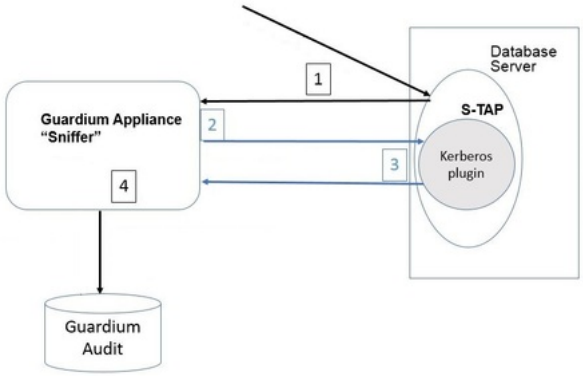
Kerberos es un protocolo de autenticación de red que elimina la transmisión de contraseñas no cifradas a través de la red. Funciona en una modalidad de autenticación mutua, que verifica tanto la identidad del usuario que solicita autenticación como las del servidor que proporciona la autenticación solicitada. El mecanismo de autenticación de Kerberos emite certificados para acceder a los servicios de red. Estos certificados contienen datos cifrados, incluida una contraseña cifrada, que confirma la identidad del usuario ante el servicio solicitado.

Para la auditoría y emisión de alertas, es importante saber el usuario de la base de datos que ha realizado una acción. Cuando se realiza el inicio de sesión con un certificado de Kerberos, la determinación del usuario de la base de datos no siempre es sencilla.

Guardium S-TAP sólo ve el tráfico de red y lo pasa al sniffer del dispositivo Guardium. Cuando se utiliza un certificado de Kerberos para el inicio de sesión, S-TAP pasa ese certificado de Kerberos junto con el sniffer. Para algunos tipos de servidor de base de datos, el sniffer puede determinar el usuario de la base de datos a partir del tráfico de inicio de sesión de Kerberos y no es necesaria ninguna información adicional. Para otros tipos de servidor de base de datos, el sniffer necesita ayuda. Esa función la lleva a cabo el plugin de S-TAP Kerberos.

El plugin de S-TAP Kerberos no está habilitado de forma predeterminada; requiere configuración adicional.

Si utiliza Kerberos, configure el plugin. La configuración del plugin, si lo necesita, no afecta al rendimiento.



El flujo de datos entre la base de datos, el sniffer de Guardium y los datos de auditoría de Guardium es:

1. S-TAP captura el paquete de inicio de sesión de base de datos de Kerberos (junto con otra actividad) y lo envía al dispositivo Guardium.
2. Si el sniffer puede determinar el nombre de usuario a partir del certificado de Kerberos, lo analiza.
3. Si el sniffer no puede determinar el nombre de usuario a partir del certificado de Kerberos, envía el certificado de Kerberos, junto con una solicitud para el usuario de la base de datos, a S-TAP. S-TAP realiza una comprobación para ver si hay un plugin de Kerberos configurado. Si hay un plugin configurado de Kerberos, S-TAP da el certificado al plugin y el plugin intenta averiguar el DB_USER a partir del certificado. Devuelve el nombre del usuario de la base de datos a S-TAP. (Si no es así, el nombre del usuario de la base de datos no se suministra y el usuario no ve los nombres del usuario de la base de datos en los informes).
4. Ahora el sniffer puede llenar el usuario de la base de datos correspondiente a dicho certificado y correlacionarlo con el resto de la actividad de base de datos para ese usuario en la auditoría.

- Autenticación Kerberos: bases de datos soportadas
  Vea la lista de servidores de base de datos que reciben soporte para la autenticación de Kerberos y si necesitan el plugin de Kerberos.
- Habilitación del plugin de Kerberos
- Configuración del plugin de Kerberos
  Para supervisar el tráfico de la base de datos en un servidor que utiliza la autenticación de Kerberos, incluida la identificación de DB_USER, debe configurar los archivos guardtap.ini y guardkerbplugin.conf correctamente.
- Búsqueda de los parámetros de configuración de Kerberos para Oracle
  Para Oracle Kerberos, localice la tabla de claves de Kerberos y las ubicaciones de los archivos de configuración en sqlnet.ora.
- Búsqueda de los parámetros de configuración de Kerberos para Sybase
  Utilice las variables de entorno de Sybase para obtener la información de Kerberos.

Tema principal: S-TAPs y otros agentes

Autenticación Kerberos: bases de datos soportadas

Vea la lista de servidores de base de datos que reciben soporte para la autenticación de Kerberos y si necesitan el plugin de Kerberos.

Base de datos	¿Se necesita el plugin de Kerberos?
DB2	No
Oracle	Sí
Cassandra	Sí
Sybase ASE	Sí
HBase	Sí
MongoDB	No
HDFS	No

Base de datos	¿Se necesita el plugin de Kerberos?
Big SQL	No
Hive	Sí
Impala	No

Tema principal: Tráfico de base de datos autenticado mediante Kerberos

Habilitación del plugin de Kerberos

Acerca de esta tarea

Para habilitar el plugin, edite el archivo de configuración guard_tap.ini y cambie la entrada **kerberos_plugin_dir** para que apunte al directorio en el que se encuentra el propio plugin (libguardkerbplugin.so) y el archivo de configuración (guardkerbplugin.conf).

Procedimiento

1. Para una instalación predeterminada del shell: `kerberos_plugin_dir=/usr/local/guardium/guard_stap`
2. Para una instalación predeterminada de GIM: (la vía de acceso exacta varía según el release de software que se utilice)
   `kerberos_plugin_dir=/usr/local/IBM/modules/STAP/10.1.3_r101299_1-1495145548`
3. Predeterminado (el plugin está inhabilitado): `kerberos_plugin_dir=NULL`

Tema principal: Tráfico de base de datos autenticado mediante Kerberos

Configuración del plugin de Kerberos

Para supervisar el tráfico de la base de datos en un servidor que utiliza la autenticación de Kerberos, incluida la identificación de DB_USER, debe configurar los archivos guardtap.ini y guardkerbplugin.conf correctamente.

Acerca de esta tarea

Todos los valores de personalización para el plugin de Kerberos se encuentran en el archivo guardkerbplugin.conf. El contenido predeterminado de este archivo es:

```
# Kerberos values
KRB5RCACHETYPE=none
KRB5_KTNAME=/path/to/kerberos/krb5.keytab
KRB5_CONFIG=/path/to/kerberos/krb5.conf
# Plugin values
KRB5_PLUGIN_CCACHE=/path/to/kerberos/krb5cc_*
KRB5_PLUGIN_GSSAPI_LIBRARY=/path/to/lib/libgssapi_krb5.so
#KRB5_PLUGIN_DEBUG=0
```

Las líneas que empiezan con un #, así como las líneas en blanco, se tratan como comentarios y, por lo tanto, son ignoradas. Las entradas no válidas originarán un error e impedirán la ejecución del plugin de Kerberos.

Cuando se cambia una entrada de configuración, se debe iniciar el S-TAP para que los cambios se hagan efectivos.

Las entradas de configuración son:

KRB5RCACHETYPE
: `KRB5RCACHETYPE=none`

KRB5_KTNAME
: Se trata de la vía de acceso al archivo keytab. Puede tratarse de un archivo keytab que el sistema ya esté utilizando, o uno para que lo utilice el plugin generado específicamente por los programas de utilidad de Kerberos. En general, el nombre de este archivo es krb5.keytab. Por ejemplo:
  `KRB5_KTNAME=/home/oracle11/krb5/keytabKRB5_KTNAME=/home/sybase15/kerberos/keytab`

KRB5_CONFIG
: Se trata de la vía de acceso al archivo de configuración de Kerberos que utiliza el sistema. En general, el nombre de este archivo es krb5.conf. Por ejemplo:

  `KRB5_CONFIG=/home/oracle11/krb5/krb5.conf KRB5_CONFIG=/home/sybase15/kerberos/krb5.conf`

KRB5_PLUGIN_CCACHE
: Es una vía de acceso con comodines a la ubicación en la que se encuentran los archivos de caché del sistema Kerberos. Se pueden especificar varias vías de acceso separadas símbolos de punto y coma (';'). Por ejemplo
  `KRB5_PLUGIN_CCACHE=/tmp/krb5cc* KRB5_PLUGIN_CCACHE=/home/sybase16/krb5cc*;/tmp/krb5cc*`
  Nota: Especificar más archivos que los necesarios (por ejemplo, especificando /tmp/*) afectará al rendimiento.

KRB5_PLUGIN_GSSAPI_LIBRARY
: Se trata de la ubicación de la biblioteca dinámica GSSAPI de Kerberos. En la mayoría de los sistemas será libgssapi_krb5.so.

  La ubicación se puede especificar mediante una vía de acceso completa; por ejemplo

  `KRB5_PLUGIN_GSSAPI_LIBRARY=/usr/lib64/libgssapi_krb5.so KRB5_PLUGIN_GSSAPI_LIBRARY=/opt/freeware/lib64/libgssapi_krb5.so`

  Como alternativa, si la biblioteca se encuentra en la vía de acceso de búsqueda de bibliotecas estándar para el sistema, sólo se debe especificar el nombre; por ejemplo

  `KRB5_PLUGIN_GSSAPI_LIBRARY=libgssapi_krb5.so`
  Nota: También se deben encontrar en el sistema todas las bibliotecas necesarias para GSSAPI (habitualmente libkrb5.so, libk5crypto.so y libkrbsupport.so).

KRB5_PLUGIN_DEBUG
: Este parámetro solo se utiliza para la depuración del plugin. En el funcionamiento habitual, esta línea debe estar comentada, de lo contrario, el rendimiento se verá afectado.

Procedimiento

1. En el archivo guard_tap.ini, cambie el valor del parámetro kerberos_plugin_dir por la vía de acceso completa a Guardium S-TAP, ya que es donde se encuentra el plugin.
   - Instalación de GIM: kerberos_plugin_dir=<guardium_base>/modules/STAP/current
   - Instalación del shell de S-TAP: kerberos_plugin_dir=<guardium_base>/guard_stap
2. Configure estos valores en el archivo guardkerbplugin.conf, que también se encuentra en el directorio de instalación de S-TAP:
   - KRB5_KTNAME=<vía de acceso completa al archivo krb5.keytab de kerberos>
   - KRB5_CONFIG=<vía de acceso completa al archivo krb5.conf de kerberos>
   - Parámetro de configuración opcional para el caché de ticket. Este parámetro puede ser necesario si el plugin de Kerberos no reconoce el usuario. Este parámetro acepta caracteres comodín, ya que normalmente hay más de un archivo de memoria caché. Se pueden especificar varias vías de acceso separadas por dos puntos. KRB5_PLUGIN_CCACHE=<vía acceso completa a archivos krb5cc_*:vía de acceso adicional a archivos krb5cc_*:etc>

   Nota: En releases de Guardium anteriores a V. 10.1.2, los parámetros allow_weak_crypto = 1 y clockskew = 600 son obligatorios. En la mayoría de los casos, estos parámetros ya no son necesarios

Tema principal: Tráfico de base de datos autenticado mediante Kerberos

Búsqueda de los parámetros de configuración de Kerberos para Oracle

Para Oracle Kerberos, localice la tabla de claves de Kerberos y las ubicaciones de los archivos de configuración en sqlnet.ora.

Acerca de esta tarea

Procedimiento

1. Escriba: ~]$ grep –i KERBEROS $ORACLE_HOME/network/admin/sqlnet.ora
   El resultado es parecido al siguiente:

```
SQLNET.AUTHENTICATION_KERBEROS5_SERVICE = oracle
SQLNET.KERBEROS5_CONF = /home/oracle11/krb5/krb5.conf
SQLNET.KERBEROS5_REALMS = /home/oracle11/krb5/krb.realms
SQLNET.AUTHENTICATION_SERVICES= (BEQ,KERBEROS5)
SQLNET.KERBEROS5_CLOCKSKEW = 600
SQLNET.KERBEROS5_KEYTAB = /home/oracle11/krb5/keytab
SQLNET.KERBEROS5_CONF_MIT = TRUE
```

2. Para encontrar el parámetro cache de Kerberos, escriba: ~]$ oklist|grep -i cache

   El resultado es parecido al siguiente:

```
Ticket cache: /tmp/krb5cc_500
```

Tema principal: Tráfico de base de datos autenticado mediante Kerberos

Búsqueda de los parámetros de configuración de Kerberos para Sybase

Utilice las variables de entorno de Sybase para obtener la información de Kerberos.

Procedimiento

1. Escriba: klist -k
   El resultado es parecido al siguiente:

```
env|grep -i KRB
KRB5_KTNAME=/home/sybase15/kerberos/keytab
KRB5_CONFIG=/home/sybase15/kerberos/krb5.conf
```

2. Para encontrar el parámetro cache de Kerberos, escriba: klist -c

   El resultado es parecido al siguiente:

```
Ticket cache: FILE:/tmp/krb5cc_533
```

Tema principal: Tráfico de base de datos autenticado mediante Kerberos

Utilización de bibliotecas de salida

Las bibliotecas de salida incluyen una biblioteca de Guardium en la base de datos, utilizando el mecanismo de salida. La biblioteca, o módulo, de salida permite la comunicación directa entre el S-TAP de Guardium para reenviar el tráfico de la base de datos.

- Integración de DB2 Exit con S-TAP
  El mecanismo de salida de DB2 permite que Guardium seleccione todo el tráfico local o remoto de DB2 ya sea cifrado o no cifrado. No precisa de A-TAP ni de K-TAP.
- Integración de Informix Exit con S-TAP de UNIX
  El programa de utilidad Informix Exit ifxguard (Informix 12.10 y superior) supervisa conexiones a bases de datos de Informix.
- Integración de Teradata Exit con STAP de UNIX
  El módulo de salida de Teradata permite que Guardium seleccione todo el tráfico, local o remoto de Teradata ya sea cifrado o no cifrado. No precisa de A-TAP ni de K-TAP.

Tema principal: S-TAPs y otros agentes

Integración de DB2 Exit con S-TAP

El mecanismo de salida de DB2 permite que Guardium seleccione todo el tráfico local o remoto de DB2 ya sea cifrado o no cifrado. No precisa de A-TAP ni de K-TAP.

Acerca de esta tarea

La salida de DB2 incluye la biblioteca de Guardium en DB2 a través del mecanismo DB2_Exit. DB2_Exit se comunica directamente con el S-TAP de Guardium para reenviar todo el tráfico local y remoto de DB2, cifrado o no. La salida de DB2 captura tanto el tráfico TCP como el tráfico SHM. La habilitación de la cadena de UID con DB2 consume muchos menos recursos de CPU que la cadena de UID y KTAP.

La biblioteca de salida de DB2 es una biblioteca enlazada dinámica. La base de datos de DB2 carga cuando se inicia la base de datos. La biblioteca de salida de DB2 proporciona una API para la base de datos para pasar información de la sesión abierta, lecturas, escrituras y cierre.

La salida de DB2 da soporte a un cortafuegos (desde STAP 10.1.2, también precisa de DB2 versión 10.1 o posterior), terminación y cadena de UID.

Si no hay otro motor de inspección (IE) en el S-TAP que precise de KTAP, no es necesario cargar el KTAP: establezca ktap_installed=0 en guard_tap.ini o con GIM establezca ktap_enabled en no, en el diálogo de GIM para dicho STAP. También puede actualizar el SO Linux y el STAP sin tener que preocuparse de la compatibilidad de módulos de KTAP. Sin embargo, si hay otro motor de inspección (IE) en el S-TAP que precise del módulo KTAP, debe asegurarse de que haya un módulo de KTAP compatible al actualizar su versión de Linux.

Nivel de depuración de S-TAP: Con el nivel de registro de S-TAP establecido en 10, la información de depuración se registra tanto en el registro de STAP como en db2diag.log. Con un nivel de registro de 11, la información de depuración solo se registra en db2diag.log. El módulo DB2 Exit realiza el registro. Este módulo lo carga DB2. Los diagnósticos se redirigen a los archivos de registro. Puesto que técnicamente es el servidor de base de datos quien realiza el registro, hay algún impacto, dependiendo del alcance de la creación de lo registros. Tenga en cuenta que la creación de registros de STAP está pensado para la resolución de problemas y no se debería ejecutar de forma continuada.

Limitaciones:

- DB2-Exit no da soporte al enmascaramiento de datos de Guardium (limieza/redacción)
- El cortafuegos de Guardium (versión 10.1.2 y posterior) precisa de DB2 versión 10.1 o posterior.
- Procedimientos almacenados: DB2-Exit supervisa los procedimientos almacenados. Dado que Guardium no sabe lo que hay en el procedimiento almacenado, no se captura el SQL del procedimiento.

Al actualizar STAP y DB2

1. Detenga DB2.
2. Actualice el STAP.
3. Copie la última biblioteca de salida de db2 en el directorio commexit de DB2.
4. Inicie DB2.

Al aplicar parches a STAP.

1. Detenga DB2.
2. Aplique parches a la base de datos DB2.
3. En caso de que se sobrescriba la configuración de DB2 la deberá habilitar de nuevo con el mandato `db2 UPDATE DBM CFG USING COMM_EXIT_LIST libguard_db2_exit_64`
4. Inicie DB2.

El instalador de Guardium tiene dos versiones de la biblioteca DB2 EXIT: 32 y 64 bits. Utilice la que coincida con la de su instancia de DB2 instalada. Ambas versiones están el directorio de instalación de Guardium en el subdirectorio lib. En servidores Linux, la versión de 64 bits se encuentran en lib64.

Las versiones de DB2 V101FP4 y V105FP3 dan soporte a la cadena de UID.

Nombre de las bibliotecas

- libguard_db2_exit_32.so
- libguard_db2_exit_64.so

Procedimiento

1. Determine la operación a nivel de bits (bitwise) de DB2. Inicie una sesión como `root` y ejecute `db2level`. La salida es similar a `DB21085I Instance db2inst1 uses 64 bits and DB2 code release SQL09070, with level identifier 08010107`
2. Localice la ubicación de la biblioteca de salida de almacenamiento intermedio de comunicaciones (DB2PATH)
   a. Inicie una sesión como usuario DB2 `trip`
   b. El procesador de línea de mandatos de DB2, ejecute db2 `get database manager configuration`
   c. En la salida, busque la vía de acceso de base de datos predeterminada:
   `(DFTDBPATH) = /DB2/trip`
   DFTDBPATH es el valor que necesita para el parámetro de entorno DB2PATH.
3. Configure la biblioteca DB2 Exit.
   a. Inicie una sesión como usuario `root`
   b. Establezca el parámetro de entorno: `# export DB2PATH=/DB2/trip`
   c. Cree el directorio especificando uno de estos mandatos. (Esto sólo se hace la primera vez que se instala la biblioteca, ya que el directorio no existe)
      - mkdir $DB2_PATH/sqllib/security/plugin/commexit
      - mkdir $DB2_PATH/sqllib/security64/plugin/commexit
   d. Cambie los permisos: `# chown ${DB2 user}:${DB2 group} $DB2PATH/security64/plugin/commexit`
   e. Copie el archivo libguard de Guardium especificando uno de los siguientes mandatos:
   ```
   # cp /opt/IBM/guardium/module/modules/STAP/libguard_db2_exit_64.so $DB2PATH/security64/plugin/commexit
   # cp /opt/IBM/guardium/module/modules/STAP/libguard_db2_exit_64.so $DB2PATH/security/plugin/commexit
   ```
   donde $DB2_PATH es el directorio de instalación de db2.

   Si la copia falla con el error `....: Text file busy`, quítelo del directorio de destino, realice una copia y repita.

   f. Cambie los permisos especificando uno de los siguientes mandatos:
   ```
   # chown ${DB2 user}:${DB2 group} $DB2PATH/security64/plugin/commexit/libguard_db2_exit_64.so
   # chown ${DB2 user}:${DB2 group} $DB2PATH/security/plugin/commexit/libguard_db2_exit_64.so
   ```
4. Añada la instancia de DB2 al grupo de Guardium. El grupo de Guardium se crea durante la instalación de S-TAP. Este requisito aumenta la seguridad de las regiones de memoria compartida creadas por el S-TAP.

a. Si el usuario DB2 es 'trip', verifique si 'trip' ya ha sido autorizado. Utilice guardctl bajo la carpeta del ATAP. #
```
/opt/IBM/guardium/module/modules/ATAP/10.1.0_r88469_1-1468880597/files/bin/guardctl is-user-authorized trip
User 'trip' is authorized.
```
b. Si el usuario trip no está autorizado, autorícelo ahora:
```
# /opt/IBM/guardium/module/modules/STAP/10.1.0_r88469_1-1468880597/guardctl authorize-user trip
guardctl authorize-user guardium
User 'guardium' is already authorized.
```

5. Habilite la salida de db2 en DB2 (de esta forma enviará el tráfico SQL al S-TAP).
   a. Inicie una sesión como usuario de db2 y utilice los mandatos del procesador de línea de mandatos de db2 para habilitarla:
   ```
   db2 UPDATE DBM CFG USING COMM_EXIT_LIST libguard_db2_exit_64
   ```
   b. Una vez habilitada, db2 envía tráfico SQL al STAP. Verifique si la salida de db2 está habilitada correctamente especificando
   ```
   db2 get database manager configuration
   ```
   La salida debería incluir:
   ```
   Communication buffer exit library list (COMM_EXIT_LIST) = libguard_db2_exit_64
   ```
6. Reinicie DB2.
   a. Inicie una sesión como usuario de db2 y reinicie la base de datos tal como se indica a continuación:
   ```
   # db2stop force; ipclean; db2start
   ```
   b. Verifique que la respuesta incluye
   ```
   The DB2START command completed successfully
   ```
   c. Si la acción de reiniciar no acaba de forma satisfactoria, detenga la salida de db2 para borrar los avisos en DB2 especificando:
   ```
   db2 UPDATE DBM CFG USING COMM_EXIT_LIST NULL
   ```
   y reinicie con
   ```
   db2 restart
   ```
   d. Si no, consulte el archivo de registro para averiguar la causa: ~/sqllib/db2dump/db2diag.log
7. Si el A-TAP no está activado: Configure STAP para DB2_EXIT. (Si A-TAP está activado, continué con 8)
   a. Configure el motor de inspección (IE) para DB2 de la forma habitual en guard_tap.ini o a través de GIM. Para facilitar la identificación, establezca db_type=db2.
   b. Solo plataformas de tipo Linux: Verifique que el parámetro db_install_dir para DB2_EXIT IE se establece en el valor de la variable de entorno de DB2 $DB2_HOME o $HOME.
   c. Solo Windows: Añada instance_name=Nombre_servicio. Determine el nombre de servicio con el programa de utilidad db2tap en la carpeta de instalación del S-TAP, o desde el panel de control. Establezca el nombre de instancia en la parte del nombre de servicio que hay detrás del segundo delimitador de guión (-). Por ejemplo, si el nombre del servicio en el panel de control es DB2 - DB2COPY1 - DB2-01-0, establezca INSTANCE_NAME en DB2-01-0.
   d. Reinicie el STAP con la nueva configuración.
8. Si se activó un A-TAP al iniciar.
   a. Detenga DB2 especificando
   ```
   # db2stop force;ipclean
   ```
   b. Desactive el ATAP especificando
   ```
   # /opt/IBM/guardium/module/modules/ATAP/10.1.0_r88469_1-1468880597/files/bin/guardctl db_instance=<instancia_bd> [--
   force-action=yes ] deactivate
   ```
   c. Configure el motor de inspección (IE) para DB2 de la forma habitual en guard_tap.ini o a través de GIM. Para facilitar la identificación, establezca db_type=db2.
   d. Solo plataformas de tipo Linux: Verifique que el parámetro db_install_dir para DB2_EXIT IE se establece en el valor de la variable de entorno de DB2 $DB2_HOME o $HOME.
   e. Solo Windows: Añada instance_name=Nombre_servicio. Determine el nombre de servicio con el programa de utilidad db2tap en la carpeta de instalación del S-TAP, o desde el panel de control. Establezca el nombre de instancia en la parte del nombre de servicio que hay detrás del segundo delimitador de guión (-). Por ejemplo, si el nombre del servicio en el panel de control es DB2 - DB2COPY1 - DB2-01-0, establezca INSTANCE_NAME en DB2-01-0.
   f. Reinicie el STAP con la nueva configuración.
9. Establezca zonas/WPAR.
   a. Copie el S-TAP para zonas/wpars
      i. En la WPAR/zona global/maestro: (suponiendo que el software de Guardium está instalado en la WPAR/zona maestra bajo /usr/local/guardium y que exista un directorio /usr/local el que se pueda escribir con el suficiente espacio libre en la sub-zona/sub-WARP), especifique:
      ```
      cd /usr/local
      tar -cvf - guardium | ssh root@subzonehost 'cd /usr/local && tar -xvf -'
      ```
      ii. En las zonas/WPAR, añada DB2_EXIT IE en guard_tap.ini con:
      - -- ktap_installed = 0
      - -- tap_run_as_root = 1
      - -- tap_ip = dirección IP local de zonas/wpar
      - No se debe especificar ningún otro motor de inspección (IE) para iniciar el S-TAP en la zona.

   b. Cree el directorio /var/guard.
   c. Inicie el S-TAP.
      - Las WPAR, añada/copie manualmente la entrada del servidor utap en el archivo inittab.
      - En Solaris siga la siguiente información en este enlace: https://scm.guard.swg.usma.ibm.com/wiki/index.php?page=Use_Solaris_services
   d. Siga las instrucciones en la configuración inicial.
   e. Seleccione el nivel de registro.
      Nota: **Impacto de la creación de registros de depuración en el servidor de base de datos:**La creación de registros se realiza mediante el módulo DB2 Exit. Este módulo lo carga DB2. Los diagnósticos se redirigen a los archivos de registro. Puesto que es el servidor de base de datos quien técnicamente realiza el registro, hay un cierto impacto que depende de la cantidad de información que se registre. Recuerde que la creación de registros de STAP está pensada para resolver problemas y no como una característica estándar, por lo que el impacto sólo se da cuando se activa la creación de registros.
      - Cuando el nivel de registro de S-TAP = 10, la información de depuración se registra tanto en el registro de S-TAP como en el de db2_exit (db2diag.log)
      - Cuando el nivel de registro de S-TAP = 11, la información de depuración solo se registra en el registro de db2_exit (db2diag.log)

Nota: En un entorno WPAR en el que se ejecuta el descubrimiento, si el nombre de la instancia es la misma en la zona esclava y en la maestra, solo se añade la entrada del motor de inspección que pertenece a la zona maestra.
Nota: Cuando se modifica tap_identifier en el motor de inspección, para que el cambio entre en vigor con Informix Exit o DB2 Exit, se tendrá que reiniciar la base de datos. Con ATAP habilitado, será necesario detener la base de datos, desactivar ATAP, reactivarlo y finalmente volver a iniciar la base de datos para que tap_identifier funcione para DB2 Exit e Informix Exit; asegúrese de que db_install_dir es exactamente el mismo valor que $HOME en la base de datos. Además se tiene que reiniciar la base de datos para que adopte el valor de tap_identifier. Para Informix Exit, detenga ifxguard y, a continuación, reinicie la base de datos y luego inicie ifxguard.

Tema principal: Utilización de bibliotecas de salida

Integración de Informix Exit con S-TAP de UNIX

El programa de utilidad Informix Exit ifxguard (Informix 12.10 y superior) supervisa conexiones a bases de datos de Informix.

Acerca de esta tarea

Con Informix Exit, Guardium v.10 y posterior puede auditar todos los protocolos de las actividades SQL de Informix. Incluye los protocolos TCP, de memoria compartida y de conductos con nombre. Se da soporte a todas las características de Guardium (S-Gate, cadenas UID, redacción, reescritura de consultas, etc.). En las plataformas Linux, puede utilizar Informix Exit en lugar de utilizar ATAP para capturar tráfico de memoria compartida. La salida de Informix captura tráfico cifrado.

El programa de utilidad ifxguard está bajo $INFORMIXDIR/bin. Una biblioteca compartida, Informix Exit, es parte de la instalación del S-TAP de Unix de Guardium. ifxguard lo carga en tiempo de ejecución. S-TAP incluye 32bit y 64bit.so. Las bibliotecas estáticas también son inclusivas. Se encuentran ubicadas bajo <directorio_instalación_guardium>/guard_stap, por ejemplo:
/usr/local/guardium/guard_stap /usr/local/guardium/guard_stap/libguard_informix_exit_32.so
/usr/local/guardium/guard_stap/libguard_informix_exit_64.so.

Nota: Cuando se modifica tap_identifier en el motor de inspección, para que el cambio entre en vigor con Informix Exit o DB2 Exit, es necesario reiniciar la base de datos. Con ATAP habilitado, es necesario detener la base de datos, desactivar ATAP, reactivarlo y finalmente volver a iniciar la base de datos. Para que tap_identifier funcione para las salidas de DB2 e Informix; asegúrese de que el valor de db_install_dir coincida con el valor de $HOME en la base de datos. Además se tiene que reiniciar la base de datos para que adopte el valor de tap_identifier. Para Informix Exit, detenga ifxguard y, a continuación, reinicie la base de datos y luego inicie ifxguard.

Procedimiento

1. Inicie una sesión como usuario informix en la base de datos y localice el nombre de la instancia (INFORMIXSERVER) y su directorio de instalación (INFORMIXDIR) ejecutando estos mandatos Unix:
```
$ echo $INFORMIXSERVER
INFORMIXSERVER=test117
$ echo $INFORMIXDIR
INFORMIXDIR=/home/informix
```
2. Instale e inicie el S-TAP en el host de base de datos. Consulte Instale el cliente de S-TAP en un servidor Linux, Solaris, AIX o HP-UX.
3. Como usuario root, asegúrese de que el usuario informix está en el grupo guardium, por ejemplo,
```
/usr/local/guardium/bin/guardctl authorize-user informix
```
o con unix
```
# chgroup users=informix guardium
```
(solo AIX).
4. Inicie una sesión como usuario informix y especifique:
```
$ iduid=501(informix) gid=205(informix) groups=215(guardium)
```
5. Como usuario informix, copie la biblioteca de salida de informix correcta desde el directorio de guard_stap en el directorio de biblioteca del usuario informix, por ejemplo,
```
cp /usr/local/guardium/guard_stap/libguard_informix_exit_64.so
$INFORMIXDIR/lib/libguard_informix.so
```
6. Configure ifxguard. Cree un archivo de configuración bajo $INFORMIXDIR/etc/ifxguard.$INFORMIXSERVER con estas líneas:
```
NAME ol_informix1210
WORKERS 2
LIBPATH /home/informix/12.10.FC6/lib/libguard_informix.so
DEBUG 1
LOGFILE /home/informix/12.10.FC6/etc/ifxguard.msg.txtg.txt
```
Nota: INFORMIXDIR=/home/informix/12.10.FC6
7. Active ifxguard como usuario informix
   a. Asegúrese de que el servidor de bases de datos de Informix está en línea (onstat -).
   ```
   $ id
   uid=501(informix) gid=205(informix) groups=215(guardium) $ onstat -
   IBM Informix Dynamic Server Version 12.10.FC6 -- On-Line -- Up 6 days 00:22:25 -- 253104 Kbytes
   ```
   b. Si el archivo de configuración de ifxguard está configurado como se acaba de describir, active ifxguard con:
   ```
   $ ifxguard
   15:20:17 ifxguard set instance name ol_informix1210
   Starting ifxguard ol_informix1210 ...
   check log file: /home/informix/12.10.FC6/etc/ifxguard.msg.txt
   ```
   No debería aparecer ningún error. En caso de que haya errores, compruebe el archivo indicado en LOGFILE.
   c. Si el archivo de configuración de ifxguard no está bajo $INFORMIXDIR/etc, especifique la vía de acceso completa al archivo con la opción -c, por ejemplo
   ```
   $ ifxguard -c /mnt/conf/ifxguard.ol_informix1210
   ```
   d. Si el archivo de configuración de ifxguard no está configurado en modo alguno, todavía tiene la posibilidad de activar el agente especificando la biblioteca .so con la vía de acceso completa con la opción -p y el archivo de registro de mensajes con la opción -l, por ejemplo
   ```
   $ ifxguard -p /home/informix/12.10.FC6/lib/libguard_informix.so -l  home/informix/12.10.FC6/etc/ifxguard.msg.txt
   ```
   e. Si hay errores, consulte el archivo de registro indicado en LOGFILE.
8. Asegúrese de que ifxguard y S-TAP están en ejecución con la ayuda de ps -ef:
```
$ ps -ef|grep guard
root 15401210 1 1 15:14:11 - 0:00
/usr/local/guardium/guard_stap/guard_stap /usr/local/guardium/guard_stap/guard_tap.ini
informix 22609968 1 0 15:20:17 - 0:00 ifxguard
```

Debería ver el siguiente mensaje en /home/informix/12.10.FC6/etc/ifxguard.msg.txt.

```
Wed Feb  3 15:20:17 2016
15:20:17 INFORMIX-ESQL Version 12.10.FC6
15:20:17 Build Number:  N253
15:20:17 Build Host:    cxp01007
15:20:17 Build OS:      AIX 6.1
```

```
15:20:17 Build Date:    Wed Nov 4 21:55:13 CST 2015
15:20:17 GLS Version:   glslib-6.00.FC7
15:20:17
15:20:17 Starting ifxguard ol_informix1210 ...
15:20:17 DEBUG[TID1]:Password File /home/informix/12.10.FC6/etc/ passwd_file failed error:No
such file or directory [2] [onguard_main.c:onguard_pw_init:518]
15:20:17 DEBUG[TID1]:ifxguard ol_informix1210 connect to trusted host, Password Manager is i
gnored. [onguard_main.c:onguard_run:2391]
15:20:17 pcbms = 110023688, spt_fn=fffffffffffff300

15:20:17 CBMS: cbms_initialize()
15:20:17 Attached /.guard_writer0 shmem[0] 8001000a0000de8
15:20:17 Attached /.guard_writer1 shmem[1] 8001000a0000eb8
15:20:17 Attached /.guard_writer2 shmem[2] 8001000a0000f88
15:20:17 Attached /.guard_writer3 shmem[3] 8001000a0001058
15:20:17 Attached /.guard_writer4 shmem[4] 8001000a0001128
15:20:17 Attached /.guard_writer5 shmem[5] 8001000a00011f8
15:20:17 Attached /.guard_writer6 shmem[6] 8001000a00012c8
15:20:17 Attached /.guard_writer7 shmem[7] 8001000a0001398
15:20:17 Attached /.guard_writer8 shmem[8] 8001000a0001468
15:20:17 Attached /.guard_writer9 shmem[9] 8001000a0001538
15:20:17 Attached to /.guard_reader
15:20:17 guard_conf_message=70000000149b000: my_ip=96eb8b7, intercept_type=1c, debug_level=0
, ignore_response_db_list=NONE
15:20:17 comm exit shm initialization successful
15:20:17 DEBUG[TID1]:new daemon pid is 22609968 [onguard_main.c:onguard_daemonize:2350]
15:20:17 ifxguard ol_informix1210 started
15:20:17 The connection attempt from  ifxguard ol_informix1210 to server ol_informix1210 suc
ceeded. Process id: 22609968:258
15:20:17 Attached to /.guard_reader
15:20:17 The connection attempt from  ifxguard ol_informix1210 to server ol_informix1210 succeeded. Process id: 22609968:515
```

Puede ignorar el **error de archivo de contraseñas**. Se trata de un mensaje de depuración. Puede definir un archivo de contraseñas y ejecutar 'onpassword' para cifrarlo. Ifxguard lee la contraseña de informix de usuario desde el archivo cifrado y se conecta a IDS (Informix Dynamic Server). Si no hay definido un archivo de contraseñas, ifxguard se conecta a IDS como una conexión de host de confianza (sin contraseña).

9. Añada el motor de inspección INFX_EXIT a través de la GRDAPI (create_stap_inspection_engine) o desde la interfaz gráfica de usuario (Gestionar > Supervisión de actividad > Control de S-TAP) con estos valores específicos de Informix:

Parámetro de GUI	Parámetro en GRDAPI	Valor
Protocolo	protocol	Informix Exit
Dir de instalación de BD	dbInstallDir	/home/informix
Nombre de proceso	procName	/INFORMIXTMP/.inf.sqlexec
Tipos de interceptación	interceptTypes	<blanco o nulo>
Identificador	ieIdentifier	<blanco o nulo>
	informixVersion	Versión de Informix

10. Reinicie el S-TAP.
11.
12. Para inhabilitar libguard, ejecute: ifxguard -kill $INFORMIXSERVER

Tema principal: Utilización de bibliotecas de salida

Integración de Teradata Exit con STAP de UNIX

El módulo de salida de Teradata permite que Guardium seleccione todo el tráfico, local o remoto de Teradata ya sea cifrado o no cifrado. No precisa de A-TAP ni de K-TAP.

Acerca de esta tarea

S-TAP en Teradata 16.10 y superior precisa esta configuración.

La salida de Teradata incluye la biblioteca de Guardium en DB2 a través del módulo de salida. El módulo de salida se comunica directamente con el S-TAP de Guardium para reenviar todo el tráfico de Teradata.

La salida de Teradata da soporte a terminación y cortafuegos. No da soporte a la redacción ni a la cadena de UID.

La ubicación de libguard_teradata_exit_64.so y otros archivos de Guardium varia en función del método de instalación y del directorio elegidos.

Procedimiento

1. Configure el motor de inspección (IE) de Teradata Exit en el guard_tap.ini local, de forma parecida a lo que se indica a continuación:

```
[DB_0]
connect_to_ip=127.0.0.1
db_exec_file=/opt/teradata/tdat/tgtw/16.00.00.05sks/bin/gtwgateway
db_install_dir=/root
db_type=trd_exit
intercept_types=NULL
tap_identifier=NULL
networks=0.0.0.0/0.0.0.0
exclude_networks=
```

2. Si edita localmente, reinicie el S-TAP.
3. Como usuario root, especifique

```
ln -s /usr/local/guardium/lib64/libguard_teradata_exit_64.so /opt/teradata/tdat/tgtw/site/libtgtwmonitoring.so
/usr/local/guardium/guard_stap/guardctl --db-user=tdatuser authorize-user
/usr/local/guardium/guard_stap/guardctl --db-user=teradata authorize-user
/usr/local/guardium/guard_stap/guardctl --db-user=root authorize-user
/usr/tgtw/bin/gtwcontrol --monitorlib load=yes
```

4.

Tema principal: Utilización de bibliotecas de salida

Configuración especial de entornos Linux, Solaris, HP-UX y AIX

Utilice estos procedimientos para los correspondientes sistemas con zonas, RAC, particiones de carga de trabajo (WPAR) o clústeres.

- Configuración de STAP para zonas de Solaris
  Instalar y configurar S-TAP en la zona maestra (zona global). Todas las otras zonas (locales) comparten el recurso con la zona maestra.
- Configuración de S-TAP de Oracle RAC
- Configuración de S-TAP para WPAR de DB2
- Activación de A-TAP en todos los nodos de un clúster de DB2
  Es necesario activar los A-TAP en todos los nodos donde un servidor DB2 es compartido por los nodos en un clúster de DB2.
- Configuración del montaje retardado en disco de clúster
  Este tema sólo se aplica a los servidores de base de datos Oracle, Informix y DB2.

Tema principal: S-TAPs y otros agentes

Configuración de STAP para zonas de Solaris

Instalar y configurar S-TAP en la zona maestra (zona global). Todas las otras zonas (locales) comparten el recurso con la zona maestra.

Acerca de esta tarea

Procedimiento

1. Instale S-TAP en la zona maestra (zona global) independientemente de la zona en la que se ejecute la base de datos, puesto que las zonas locales comparten información de la zona maestra.
2. Al configurar el motor de inspección (IE), utilice los valores de la zona global para la vía de acceso de db_install_dir y tap_db_process_names. (Desde la zona global, S-TAP supervisa el acceso a la base de datos en todas las zonas).
3. Si está utilizando PCAP, añada las direcciones IP de todas las zonas que desea supervisar para el parámetro alternate_ips en el archivo guard_tap.ini en la base de datos de Solaris.
4. Al final de la instalación:
   - Es visible en las zonas locales.
   - S-TAP no se ejecuta en las zonas locales.

Tema principal: Configuración especial de entornos Linux, Solaris, HP-UX y AIX

Configuración de S-TAP de Oracle RAC

Acerca de esta tarea

Oracle RAC (Real Application: Clusters) permite que varios sistemas ejecuten software de RDBMS de Oracle de forma simultánea a la vez que acceden a una única base de datos y, por lo tanto, proporciona una funcionalidad de clúster.

En una base de datos no Oracle RAC, una sola instancia accede a una sola base de datos. La base de datos consta de un conjunto de archivos de datos, archivos de control y registros redolog ubicados en el disco. La instancia consta del conjunto de la memoria relacionada con Oracle y de los procesos de sistema operativo que se ejecutan en un sistema.

En un entorno Oracle RAC, dos o más sistemas (cada uno con una instancia del RDBMS de Oracle) simultáneamente acceden a una sola base de datos. Esto permite que una aplicación o usuario se conecte a cualquiera de los sistemas y que tenga acceso a un único conjunto de datos.

Procedimiento

1. Instale S-TAP en todos los nodos. Si se utiliza GIM, instale el cliente GIM en todos los nodos y, a continuación, instale el lote S-TAP en todos los nodos.
2. Configure los parámetros de STAP. Todos los parámetros se pueden configurar mediante la interfaz de usuario de GIM.
   - STAP_TAP_IP: IP pública configurada para el nodo
   - STAP_ALTERNATE_IPS: Lista separada por comas de IP virtuales (VIP) configuradas para el nodo, y el escucha de escaneo
     Consejo: Utilice este mandato para recuperar el valor de los nombres de host virtuales para indicarlos en las alternate_ips: su – grid –c 'cat $ORACLE_HOME/network/admin/*.ora'|grep –i host

     Por ejemplo:

     ```
     [root@racvm121 ~]# su - grid -c 'cat $ORACLE_HOME/network/admin/*.ora'|grep -i host
     LISTENER_RACVM121=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=racvm121-vip.guard.swg.usma.ibm.com)(PORT=1521)
     ```

   - Configure el parámetro del motor de inspección (IE) STAP: unix_domain_socket_marker=<clave>, donde el valor de <clave> se puede encontrar en listener.ora en la definición del protocolo IPC
     Consejo: Mandato para recuperar el valor para unix_domain_socket: `su - grid -c 'cat $ORACLE_HOME/network/admin/*.ora'|grep -i KEY`
     - Ejemplo: Si aparece esta descripción en listener.ora LISTENER=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=ORCL)))) entonces unix_domain_socket_marker=ORCL
     - Ejemplo: Si hay más de una línea de IPC en listener.ora, utilice un denominador común de todas las claves:

```
su - grid -c 'cat $ORACLE_HOME/network/admin/*.ora'|grep -i KEY
LISTENER=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER))))
LISTENER_SCAN1=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER_SCAN1))))
LISTENER_SCAN2=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER_SCAN2))))
LISTENER_SCAN3=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER_SCAN3))))
```

Guardium utiliza una serie de búsqueda en la vía de acceso. "LISTENER" funciona para las cuatro y se debería utilizar en este caso: unix_domain_socket_marker=LISTENER

- Ejemplo: Si no hay un denominador común, cree motores de inspección adicionales con el unix_domain_socket_marker correspondiente a la clave o claves de IPC específicas. Por ejemplo, guard_tap.ini podría aparecer tal como se muestra al final de este ejemplo:

```
[DB_0]
...
unix_domain_socket_marker=EXTPROC1522
...
[DB_1]
...
unix_domain_socket_marker=LISTENER
```

3. Si la base de datos de Oracle está cifrada (ASO/SSL), active ATAP en todos los nodos (activos y en espera).
   a. Detenga todos los servicios Oracle (incluido el clústerware) y verifique que ohasd.bin está inactivo.
   b. Autorice a los usuarios oracle y grid (en caso de que el escucha pertenezca al usuario grid).
   c. Configure los parámetros de A-TAP utilizando la información proporcionada en la ayuda en línea o Knowledge Center.
   d. Active A-TAP.
   e. Inicie todos los servicios de Oracle en el clúster.
4. En el entorno Oracle RAC, verifique el usuario que inicia el escucha. Si se trata del usuario grid, autorícelo.

Tema principal: Configuración especial de entornos Linux, Solaris, HP-UX y AIX

Configuración de S-TAP para WPAR de DB2

Acerca de esta tarea

Cuando ktap_fast_shmem se establece en 1, si hay varias instancias de DB2 configuradas para una sola WPAR en el archivo guard_tap.ini y tienen el mismo db2_shmem_size, entonces se devolverán los valores de db2_fix_pack_adjustment y db2_shmem_client_position configurados en la primera sección de DB2 para dicha WPAR. Por lo tanto, si hay varias instancias de DB2 en ejecución en la WPAR:

- Si todas las instancias de DB2 tienen los mismos valores de db2_shmem_size, db2_fix_pack_adjustment y db2_shmem_client_position, se recopilan los paquetes de todas las instancias aunque sólo se haya configurado una instancia.
- Si todas las instancias de DB2 tienen el mismo db2_shmem_size, pero diferentes db2_fix_pack_adjustment o db2_shmem_client_position, sólo se recopilan los paquetes de la primera instancia de DB2 configurada.

Procedimiento

1. Calcule el desplazamiento del área de E/S de cliente (db2_shmem_client_position)
   a. Abra un nuevo shell bash como usuario de la instancia de db2.
   b. Ejecute el mandato ps -x para verificar que el procesador de mandatos de db2bp no se está ejecutando actualmente para este shell. No debería ver el mandato denominado db2bp en ejecución. Si lo ve, puede interrumpirlo o ejecutar un nuevo shell.
   c. Ejecute los dos mandatos siguientes:

```
db2 get database manager configuration | awk '/ASLHEAPSZ/{print $9 * 4096}'
```

   La salida es el valor necesario para db2_shmem_client_position.
2. Para encontrar el tamaño del segmento de memoria compartida de DB2 (db2_shmem_size), realice una de las siguientes acciones:
   - Este método es el que proporciona resultados más precisos.
     a. Inicie una conexión de memoria compartida de DB2 y manténgala abierta.
     b. Ejecute este mandato para obtener el ID de proceso para db2sysc: ps -eaf | grep db2sysc. La salida se parece a la siguiente:

```
db2inst1  5309370  5505772   0   Nov 11      - 1232:12 db2sysc 0
```

     En este ejemplo, el ID de proceso es 5309370.
     c. Ejecute este mandato para recuperar información sobre los procesos de memoria compartida: ipcs -ma. La salida se parece a la siguiente:

```
IPC status from /dev/mem as of Wed Nov 20 13:21:45 CST 2013
T         ID     KEY        MODE       OWNER    GROUP  CREATOR   CGROUP NATTCH     SEGSZ  CPID
m    2097152 0xffffffff D-rw------- pconsole   system pconsole   system      1 536870912 4522088
m          1 0x78000015 --rw-rw-rw-     root   system     root   system      3  16777216 3605314
m          2 0x78000016 --rw-rw-rw-     root   system     root   system      3 268435456 3605314
m  219152387 0xffffffff D-rw-------     root   system     root   system      1 536870912 5243842
m    1048580 0x61013002 --rw------- pconsole   system pconsole   system      1  10485760 4522088
m   10485765 0xd9fd8a61 --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      5  47644672 5571082
m    9437190 0xd9fd8a74 --rw-rw-rw- db2inst1 db2iadm1 db2inst1 db2iadm1      9 140852104 5571082
m    9437191 0xe1bd8858 --rw-rw----   oracle      dba   oracle      dba     40 53687107584 3801352
m    3145736 0x52594801 --rw-rw----     root informix     root informix     13 223019008 5702650
m    3145737 0xd9fd8b68 --rw-rw---- db2inst1 db2iadm1 db2inst1 db2iadm1      1  58720256 6619354
m    3145738 0xffffffff --rw------- db2fenc1 db2fadm1 db2inst1 db2iadm1      7 268435456 5505772
m         11 0x52594802 --rw-rw----     root informix     root informix     13  33439744 5702650
m         12 0x52594803 --rw-rw-rw-     root informix     root informix     13    573440 5702650
m         13 0xf2033f7e --rw------- sybase15   sybase sybase15   sybase      1 115564544 5178168
m  409993231 0x52594804 --rw-rw---- informix informix informix informix     13   8388608 5702650
m  763363344 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 268435456 5309370
m  125829140 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      2    131072 5309370
m  201326613 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 163905536 5309370
m  103750230 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 134217280 5309370
```

La salida contiene varias columnas más de las que se muestran aquí, pero no afectan a este procedimiento. Busque la línea que contiene el ID de proceso que se ha identificado en el paso 2.b y que también tiene el valor 2 bajo NATTCH. El tamaño de segmento de memoria compartida de DB2 es el valor de la columna SEGSZ. En este ejemplo, es 131072.

d. Sugerencia: si la lista devuelta en el paso 2.c es demasiado larga, puede filtrarla utilizando el ID de proceso. En este caso, debería especificar ipcs -ma | grep 5309370. Los resultados no contienen las cabeceras de columna, pero puede mirar los resultados anteriores para ver las cabeceras de columna e identificar la línea y columna correctas. En este ejemplo, es la última línea.

```
m 131072014 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 1342177280 5309370
m 763363344 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 268435456 5309370
m 227541013 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 163905536 5309370
m 106353238 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      2    131072 5309370
```

- Como alternativa, utilice este método, que es más sencillo pero menos exacto:
  ATAP y KTAP se basan en el tamaño para la identificación de los segmentos de memoria compartida de la aplicación/agente. Luego se interviene en estos segmentos mediante paquetes C2S y S2C. Los segmentos equivalen a la suma de los parámetros ASLHEAPSZ y RQRIOBLK. DB2 asigna segmentos mucho mayores. En la mayoría de los casos, el tamaño es igual a (ASLHEAPSZ + 1) * 2 páginas, o (ASLHEAPSZ + 1) * 8192 bytes. El tamaño exacto se puede determinar observando los segmentos de memoria compartidos en el sistema antes y después de que se cree una nueva conexión local de DB2. Utilice esta secuencia de mandatos para determinar el tamaño del segmento de memoria compartida. Los parámetros del mandato ipcs y el formato de salida difieren de plataforma a plataforma. El script siguiente se basa en la versión de AIX.

```
ipcs -ma | sort -n -2 +3 > /tmp/before.txt
db2 connect to <some_existing_database>ipcs -ma | sort -n -2 +3 > /tmp/after.txt
db2 terminate
diff /tmp/before.txt /tmp/after.txt | awk '{if ($10 == 2) print $11}'
```

Establezca estos parámetros con el propósito de capturar el tráfico de memoria compartida de DB2.

Tabla 1. Parámetros de DB2

Parámetro	Nombre de STAP	Nombre ATAP	Valor predeterminado	Comentario
Tamaño de cabecera de paquete	db2_fixed_pack_adjustment	db2_header_offset	20	El valor predeterminado se ha probado para DB2 8.2 y posteriores en diversas plataformas de 64 bits. Es posible que otras versiones de DB2 y plataformas de 32 bits necesiten un desplazamiento distinto. Los sospechosos habituales son 16 y 12.
Desplazamiento del área de E/S de cliente	db2_shmem_client_position	db2_c2soffset	61440	Este parámetro se deriva del parámetro DB2 ASLHEAPSZ.
Tamaño de segmento de memoria compartida de DB2	db2_shmem_size	db2_shmsize	131072	Este parámetro se determina empíricamente. Consulte una secuencia de mandatos que se puede utilizar para obtenerlo.

Tema principal: Configuración especial de entornos Linux, Solaris, HP-UX y AIX

Activación de A-TAP en todos los nodos de un clúster de DB2

Es necesario activar los A-TAP en todos los nodos donde un servidor DB2 es compartido por los nodos en un clúster de DB2.

Procedimiento

1. Autorizar al usuario de db2 en el nodo 1. <base_guardium>/xxx/guardctl authorize-user <nombre-usuario>
   Por ejemplo:

   # /usr/local/guardium/bin/guardctl authorize-user db2inst1

   # /usr/local/guardium/bin/guardctl is_user_authorized db2inst1

   User 'db2inst1' is authorized.

2. Activar A-TAP en el nodo 1.
   <base_guardium>/xxx/guardctl db_instance=<instancia> activate
   Por ejemplo:

```
# /usr/local/guardium/guard_stap/guardctl db_instance=db2inst1 activate

# /usr/local/guardium/guard_stap/guardctl list-active
db2inst1
```

3. Restaurar el servidor DB2 original en el nodo 1 después de activar el ATAP en el mismo, de forma que otros nodos puedan activar el ATAP. (Todos los nodos comparten el ejecutable. (En el directorio de administración de DB2, copie db2sysc-guard-original sobre db2sysc (realice primero una copia de cada uno y guárdelos en otro lugar). Por ejemplo:
   `# > cp db2sysc-guard-original db2sysc`
4. Suprimir el db2sysc-guard-original (o la activación fallará en el nodo 2). Por ejemplo:
   `# rm -rf db2sysc-guard-original`
5. Mover los recursos de clúster al nodo 2. Por ejemplo:
   `# pcs resource move resource_id <nodo destino>`
6. Autorizar al usuario de db2 y activar en el nodo 2 (pasos 1 y 2). Esto creará las bibliotecas en el nodo 2 y sustituirá el db2sysc-guard-original que se ha suprimido. El estado actual debería ser:
   Node01:

~]# /usr/local/guardium/guard_stap/guardctl list-active

db2inst1

Node02:

~]# /usr/local/guardium/guard_stap/guardctl list-active

db2inst1

Tema principal: Configuración especial de entornos Linux, Solaris, HP-UX y AIX

Configuración del montaje retardado en disco de clúster

Este tema sólo se aplica a los servidores de base de datos Oracle, Informix y DB2.

Para estos tipos de bases de datos, cuando se inicia el S-TAP, debe tener acceso al directorio de inicio de la base de datos. Si su entorno utiliza un esquema de clúster en el que varios nodos comparten un único disco que está montado en el nodo activo, pero no en el nodo pasivo, el directorio de inicio de la base de datos no está disponible en el nodo pasivo hasta que se produce la sustitución por anomalía.

Se puede configurar la carga retardada de S-TAP definiendo una propiedad del archivo de configuración, WAIT_FOR_DB_EXEC. Cuando se inicia, si S-TAP encuentra que no hay acceso al directorio de inicio de la base de datos, comprueba el valor de WAIT_FOR_DB_EXEC y realiza la acción adecuada.

- WAIT_FOR_DB_EXEC > 0, S-TAP se inicia independientemente de si puede stat() nombre proceso. Intenta stat () nombre proceso cada 15 minutos
- WAIT_FOR_DB_EXEC < = 0 S-TAP intenta stat() nombre proceso en el motor de inspección (IE) inmediatamente después de iniciarse. Si no puede stat() nombre proceso, S-TAP finaliza.

Antes de definir para esta propiedad un valor positivo, asegúrese de definir todas las demás propiedades de configuración necesarias y probar que S-TAP se inicia y recopila los datos correctamente. Esta propiedad solo se puede establecer editando el archivo de configuración y no desde la interfaz gráfica de usuario.

Tema principal: Configuración especial de entornos Linux, Solaris, HP-UX y AIX
Tema principal: S-TAPs y otros agentes

Guía de administración de S-TAP

Guardium S-TAP es un agente de software ligero instalado en un sistema servidor de base de datos.

S-TAP supervisa el tráfico de la base de datos y reenvía información acerca de ese tráfico a un sistema Guardium.

Visión general de S-TAP

- S-TAP puede supervisar el tráfico de la base de datos que es local con respecto a dicho sistema. Esto es importante porque las conexiones locales pueden proporcionar acceso alternativo a la base de datos y todos estos accesos se deben supervisar y auditar.
- S-TAP se puede utilizar para supervisar cualquier tráfico de red que resulte visible desde el servidor de base de datos en el que está instalado. Por lo tanto, puede actuar como recopilador en segmentos de red remotos, donde no resulta práctico instalar un sistema Guardium.
- S-TAP se puede instalar de forma remota desde la línea de mandatos en servidores Windows o Unix, además de instalarse a través de Guardium Installation Manager. Se pueden configurar actualizaciones para que se apliquen en el siguiente rearranque del servidor. En Linux, S-TAP se encarga de actualizar los componentes del kernel del S-TAP en el momento del arranque, ajustándose a las actualizaciones del kernel en entornos Linux.

Proceso de sustitución por anomalía

S-TAP recopila y envía datos a un host Guardium casi en tiempo real. S-TAP coloca los datos en el almacenamiento intermedio, para que pueda continuar funcionando si el host Guardium deja de estar disponible momentáneamente. Si el host primario no está disponible durante un largo periodo de tiempo (el tiempo puede ser más corto si el almacenamiento intermedio se llena), S-TAP puede realizar una sustitución por anomalía a un host Guardium secundario. Continuará enviando datos al host secundario hasta que el sistema Guardium deje de estar disponible, hasta que se reinicie S-TAP (que intentará conectar primero con el host primario) o hasta que se restablezca una conexión con el servidor primario y se mantenga activa durante un periodo de 5*connection_timeout_sec segundos (este valor se puede configurar en guard_tap.ini, el valor predeterminado es 10 segundos). En este caso, S-TAP realizará una sustitución por anomalía del host Guardium secundario de nuevo al host Guardium primario.

Nota: Aunque S-TAP se despliega normalmente en un servidor de base de datos, S-TAP se puede instalar en sistemas del lado del cliente como, por ejemplo, servidores de aplicaciones y clientes de base de datos.
Nota: Si S-TAP está instalado tanto en el lado de la aplicación (consulte la nota anterior) como en el servidor de base de datos, se deben tomar precauciones adicionales para no supervisar tráfico duplicado.

Sustitución por anomalía de datos de sesión

Cuando se produce una sustitución por anomalía de S-TAP, la información de sesión también se puede enviar a un host Guardium activo. Consulte el apartado sobre cómo editar el archivo de configuración de S-TAP para ver más información para definir tap_failover_session_size (0 desactivará la característica) y tap_failover_session_quiesce.

Capacidad de reinicio

Válido cuando wait_for_db_exec es mayor que 0, cuando S-TAP se reinicia, mediante un rearranque del sistema o mediante mandatos stop y start de S-TAP iniciados por el usuario, S-TAP sondea todas las bases de datos que se han configurado para su supervisión y comienza a supervisarlas cuando están disponibles. Las anomalías de configuración (ya sea en el lado de la base de datos como en el de S-TAP) que limitan la capacidad de S-TAP de supervisar una base de datos no impedirán que S-TAP supervise otras bases de datos con configuraciones válidas. En su lugar, S-TAP se iniciará correctamente, supervisará todas las configuraciones válidas y continuará sondeando otras bases de datos hasta que estén disponibles y, luego, comenzará a supervisarlas. Se recomienda que los usuarios utilicen las alertas e informes existentes para supervisar e informar sobre cualquier estado fallido.

Para Oracle, después de un reenlace el tráfico de BEQ de Oracle dejará de registrarse durante 15 minutos, que es el tiempo que tarda S-TAP en comprobar si se ha cambiado un nodo de dispositivo de Oracle.

Cortafuegos de proxy

Aunque S-TAP se despliega normalmente en un servidor de base de datos, se puede desplegar un cortafuegos basado en K-TAP en un servidor proxy. Si se establece el parámetro app_server=1 y se utiliza S-GATE, se puede supervisar el tráfico que se origina en el servidor proxy. Consulte el apartado sobre cómo editar el archivo de configuración de S-TAP y las acciones de S-GATE (acciones de bloqueo) en el tema de ayuda de políticas para obtener más información sobre cómo definir app_server y utilizar S-GATE en políticas.

Hosts de Guardium secundarios para agentes de S-TAP

Si el sistema Guardium designado como host primario para S-TAP deja de estar disponible, S-TAP puede realizar una sustitución por anomalía a un host secundario. Permanece conectado al host secundario hasta que se pierde esta conexión, hasta que se reinicia el S-TAP (que intentará primero conectarse a su host primario) o hasta que se restablece una conexión con el servidor primario durante un periodo de 5*connection_timeout_sec segundos (este valor se puede configurar en el archivo guard_tap.ini y el valor predeterminado es 10 segundos).

S-TAP se reinicia bajo condiciones ligeramente diferentes, en función del sistema operativo del servidor de base de datos:

- Unix: S-TAP se reinicia cada vez que se aplican los cambios procedentes del host activo.

Antes de designar un sistema Guardium como host secundario para un S-TAP, compruebe lo siguiente.

- El sistema Guardium debe estar configurado para gestionar los S-TAP. Para comprobarlo y volver a configurarlo si es necesario, consulte el apartado sobre cómo configurar el sistema Guardium para gestionar agentes.
- El sistema Guardium debe tener conectividad con el servidor de base de datos en el que está instalado S-TAP. Cuando se utilizan varios sistemas Guardium, a menudo se conectan a ramificaciones de la red.
- El sistema Guardium no debe tener una política de seguridad que pase por alto los datos de sesión procedentes del servidor de base de datos en el que está instalado S-TAP. En muchos casos, se incorpora una política de seguridad de Guardium para centrarse en un subconjunto reducido del tráfico observable de base de datos, pasando por alto todas las demás sesiones. Asegúrese de que el host secundario no pase por alto los datos procedentes de S-TAP o modifique la política de seguridad del sistema Guardium según sea necesario.

Para definir hosts secundarios para un S-TAP, consulte el apartado sobre cómo definir hosts Guardium secundarios para un S-TAP, en el tema sobre la configuración de los S-TAP desde la GUI.

Nota: Aunque S-TAP se despliega normalmente en un servidor de base de datos, S-TAP se puede instalar en sistemas del lado del cliente como, por ejemplo, servidores de aplicaciones y clientes de base de datos.

S-TAP y certificados

Nota: Guardium no proporciona servicios de autoridad emisora de certificados (CA) y no suministra sistemas con certificados distintos del que viene instalado de forma predeterminada. Un cliente que desee su propio certificado deberá ponerse en contacto con una entidad emisora de certificados (CA) (como, por ejemplo, VeriSign o Entrust).
Nota: Además de asegurarse de que el canal de información de S-TAP con un recopilador está cifrado, el cliente de S-TAP también se puede configurar de modo que autentique el sistema Guardium con el que está intentando comunicarse. De este modo, además de asegurar que el tráfico está cifrado, se garantiza que S-TAP no envía información a un servidor no autorizado.

Configuración de S-TAP

Para habilitar la verificación de la autenticidad del sistema Guardium, es necesario habilitar tres valores en guard_tap.ini además de use_tls=1:

1. guardium_ca_path

   Si guardium_ca_path está establecido de modo que apunte a un archivo que contiene uno o varios certificados autofirmados de CA en formato PEM, se realiza una verificación del sistema Guardium.

   Una de las CA proporcionadas en el archivo debe firmar un certificado del sistema instalado en el sistema Guardium, y el sistema Guardium debe tener la clave correspondiente correcta.

   De forma predeterminada, se proporciona un certificado root autofirmado de Guardium en la instalación de S-TAP (tanto clásica como basada en GIM). El hecho de que guardium_ca_path apunte al archivo que proporciona Guardium garantiza que el sistema Guardium tiene un par clave/certificado firmado por Guardium.

   Para utilizar claves y certificados firmados por terceros, el valor guardium_ca_path debe establecerse en un archivo que contenga los certificados de CA del tercero especificado (por ejemplo, Verisign). En este caso, el sistema Guardium debe tener el par clave/certificado firmado por el mismo tercero.

2. sqlguard_cert_cn
   Además de verificar la firma del certificado del sistema Guardium y su posesión de la clave privada correspondiente, un cliente puede optar por aceptar los certificados cuyo CN (Nombre común) no coincida con un patrón de expresión regular establecido por sqlguard_cert_cn.
   Nota: El mismo par de certificado/clave se puede instalar en varias máquinas. El cliente no tiene que comprar N certificados para N máquinas.
3. guardium_crl_path

   Si esta vía de acceso apunta a un archivo codificado con PEM con la lista de revocación de certificados de la CA, cualquier certificado del sistema Guardium que se haya revocado se rechazará. La CRL de Guardium se proporciona en la instalación de STAP (o GIM) y se actualiza mediante actualizaciones y parches de software.

   Además, un cliente puede instalar manualmente una CRL proporcionada por la entidad emisora de certificados (Guardium o un tercero).

   Puesto que no se presupone que los sistemas Guardium tienen acceso a internet, no se consulta automáticamente ningún servidor de CRL basado en la web.

Mandatos relacionados con certificados del sistema de la CLI del sistema Guardium

Existen cuatro mandatos de CLI relacionados con la gestión de certificados y claves del sistema:

- show certificate sniffer

Este mandato imprimirá el certificado del sistema en formato de texto, seguido de la codificación en formato PEM codificada en Base64. El formato de texto solo sirve para ver los detalles del certificado (en particular, el CN y el firmante/serie, que puede filtrar el S-TAP). La parte codificada en PEM comprendida entre `---BEGIN CERTIFICATE---` y `---END CERTIFICATE---` es la que se debe utilizar para hacer copia de seguridad/almacenar/enviar por correo electrónico el certificado a otras máquinas o partícipes (los delimitadores BEGIN y END siempre se deben incluir con la parte codificada en Base64).

- store certificate sniffer <console | import>

  Este mandato permite a un usuario establecer el certificado del sistema que utiliza el sistema Guardium (en comunicación con S-TAP). El certificado se puede pegar desde la consola o se puede importar a través de uno de los protocolos de importación estándar. El formato del certificado debe ser PEM y debe incluir los delimitadores BEGIN y END. Este certificado tiene que estar firmado por una entidad emisora de certificados cuyo certificado autofirmado esté disponible para el software S-TAP a través de guardium_ca_path.

- store certificate keystore <console | import>
  Este mandato permite a un usuario establecer la clave del sistema utilizada. La clave debe coincidir con la parte pública del certificado. Además, la clave tiene que estar en un sobre cifrado. La contraseña de usuario utilizada para cifrarla se debe suministrar durante el proceso de almacenamiento. El mandato store vuelve a cifrar la clave utilizando el código interno de Guardium antes de almacenarla finalmente en el sistema.
  Nota: Cuando tanto el certificado como la clave coincidente están disponibles en el sistema Guardium, S-TAP puede realizar correctamente la autenticación del sistema Guardium.
- create csr sniffer

  Este mandato se puede utilizar para crear una solicitud de firma de certificado en formato PEM. El mandato generará internamente la clave de 2048 bits y emitirá una serie de preguntas al usuario para que cumplimente el formulario de CSR (País, Estado/Provincia, Localidad/Ciudad, Organización y Unidad organizativa). Finalmente, el usuario debe proporcionar el Nombre común. Como norma general, el nombre común debe incluir sólo letras, dígitos, caracteres de subrayado y puntos. Debe ser un identificador exclusivo para una determinada instalación y debe incluir el nombre de la empresa, el departamento, el clúster o el nombre específico del sistema Guardium. Sin embargo, las instrucciones de la CA externa prevalecen sobre estas recomendaciones. Por ejemplo:

  GCluster1DataCenterGuardiumIBM - que corresponde a GCluster1 de DataCenter en Guardium, una empresa de IBM®

  SqlGuard1DataCenterGuardiumIBM - que corresponde al sistema de máquina SqlGuard1 (que también puede realizar una sustitución por anomalía)

  Especifique un correo electrónico válido cuando se le solicite, para que el personal de soporte se pueda poner en contacto con usted.

  Puede dejar los campos Contraseña de confirmación y Nombre de empresa opcional en blanco.

  Por último, la solicitud de firma de certificado se mostrará en el formulario legible y en el codificado en PEM.

  Debe verificar los detalles y enviar la parte codificada de PEM (la comprendida entre `---BEGIN CERTIFICATE REQUEST---` y `---END CERTIFICATE REQUEST----`, ambos inclusive) a la CA para que la firme.
  Nota: En este punto, el sistema tiene una clave nueva, generada internamente, que no se corresponde con el certificado de sistema instalado anteriormente. Con esto se garantiza que los S-TAP no envían información mientras el certificado se está enviando para que se firme. Si necesita garantizar un funcionamiento continuo y un canal de información de S-TAP, deberá inhabilitar la autenticación del sistema Guardium en el lado de S-TAP durante este periodo.

  Una vez que se haya verificado el CSR, la CA emitirá el certificado firmado en formato PEM. Deberá instalar este certificado mediante el mandato store system certificate.

  En este punto, el nuevo certificado y la clave generada internamente (durante el mandato create csr sniffer) coincidirán y estarán listos para ser utilizados para la autenticación del sistema Guardium por parte de los S-TAP.

  Asegúrese de que todos los parámetros relacionados con certificados del archivo de configuración de S-TAP sean correctos.

  Si tiene que instalar la misma combinación de clave/certificado en más de un sistema Guardium, puede utilizar el mandato show system certificate | key para exportarla y realizar una copia de seguridad de la misma.

  Tenga especial cuidado cuando almacene la clave (que está cifrada mediante una contraseña proporcionada por el usuario) en un dispositivo o sistema externo. Utilice contraseñas que no resulten triviales cuando se lo solicite que muestre la clave del sistema.

Tema principal: S-TAPs y otros agentes

Configuración del sistema Guardium para gestionar S-TAP

Para poder gestionar un S-TAP desde la GUI de Guardium, configure el sistema Guardium y reinicie los motores de inspección.

Acerca de esta tarea

Procedimiento

1. Finalice la sesión de Guardium.
2. Desde una ventana de cliente SSH, inicie la sesión en la interfaz de línea de mandatos (CLI) del sistema de Guardium como usuario de cli.

   ```
   ssh -l cli 192.168.2.16
   ```

   Consulte Visión general de la CLI para obtener más información sobre la utilización de la CLI de Guardium.

3. Especifique los dos mandatos siguientes:

   ```
   store unit type stap
   restart inspection-core
   ```

   Consulte los temas sobre Mandatos de CLI de configuración y control y Mandatos de CLI del motor de inspección respectivamente para obtener más información sobre estos dos mandatos.

4. Escriba quit para finalizar la sesión de la CLI de Guardium.

Tema principal: S-TAPs y otros agentes

Certificación de S-TAP

Utilice esta función para evitar que los S-TAP no autorizados se conecten al sistema Guardium.

Si hay una marca de selección en el recuadro Aprobación necesaria de S-TAP, los S-TAP no se pueden conectar hasta que se aprueben específicamente.

Si un S-TAP no aprobado se conecta, se desconectará inmediatamente hasta que alguien vaya a esta pantalla de la GUI y autorice específicamente la dirección IP de dicho S-TAP.

La función Aprobación necesaria de S-TAP se puede controlar con el mandato de la CLI store stap approval o con el mandato GuardAPI grdapi store_stap_approval.

La nueva configuración entrará en vigor después de que se ejecute el mandato restart inspection-core si utiliza el mandato de la CLI stap approval ON | OFF.

Aprobar S-TAP

1. Coloque una marca de selección en el recuadro correspondiente a Aprobación necesaria de S-TAP.
2. Especifique los clientes de S-TAP aprobados.

Nota:

Utilice la dirección IP válida, no el nombre de host.

En el entorno gestionado central, después de añadir las direcciones IP a los S-TAP aprobados, hay un tiempo de espera para la sincronización que puede tardar hasta una hora. Una vez finalizada la sincronización, el estado de los S-TAP aprobados aparecerá en verde en la GUI.

Tema principal: S-TAPs y otros agentes

Configuración de la autenticación de S-TAP con certificados SSL

Configure la autenticación entre un servidor S-TAP y el sistema Guardium.

Valor añadido: Los S-TAP se pueden configurar de modo que sólo se conecten a una determinada máquina o grupo de máquinas que se autentican con determinado certificado o conjunto de certificados. Estos certificados se pueden generar localmente en el sistema Guardium y enviarse a la entidad emisora de certificados (CA) para su firma o se pueden crear en la CA y se pueden instalar en el sistema Guardium.

Antes de empezar: Necesita saber a quién/qué/dónde actúa como su entidad emisora de certificados. Si la CA le está enviando un certificado completo para la instalación, necesita dos archivos, la clave privada en formato PKCS#8 (protegido con contraseña) y la clave pública en formato PEM. El certificado generado tiene que ser una clave RSA de 2048 bits.

Generación de la solicitud de firma de certificado (CSR) en el sistema Guardium

Inicie una sesión en el sistema Guardium con la CLI

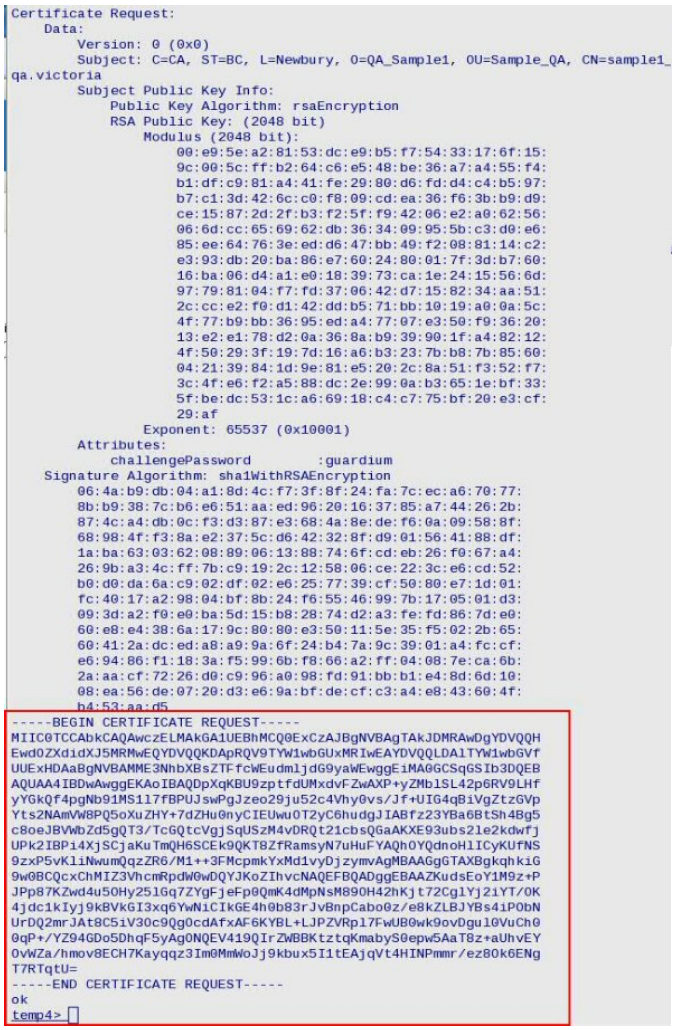
cli> create csr sniffer

[especifique los datos solicitados]

```
temp4> create system csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:CA
State or Province Name (full name) [Berkshire]:BC
Locality Name (eg, city) [Newbury]:
Organization Name (eg, company) [My Company Ltd]:QA_Sample1
Organizational Unit Name (eg, section) []:Sample_QA
Common Name (eg, your name or your server's hostname) []:sample1_qa.victoria
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

Cuando haya terminado, se mostrará algo parecido a lo siguiente:



Copie desde -----BEGIN CERTIFICATE REQUEST----- hasta -----END CERTIFICATE REQUEST----- en un archivo y envíelo a la CA para que lo firme.

La entidad emisora de certificados firmará el certificado y le enviará una clave pública.

La clave pública que envía CA tendrá un aspecto similar al siguiente:

```
enance@enance1 Latest $ cat sample1_qa.victoria.pem
-----BEGIN CERTIFICATE-----
MIID1jCCAsCgAwIBAgIBCDALBgkqhkiG9w0BAQUwgYAxCzAJBgNVBAYTAkNBMRkw
FwYDVQQIExBCcml0aXNoIENvbHVtYmlhMREwDwYDVQQHEwhWaWN0b3JpYTEUMBIG
A1UEChMLUUFfdGVzdF92aWMxFDASBgNVBAsTC1ZpY3RvcmlhX1FBMRcwFQYDVQQD
Ew5WaWN0b3JpYV9RQV9DQTAeFw0xMDExMDEyMTA5MzhaFw0xNTExMDEyMTA5Mzha
MHMxCzAJBgNVBAYTAkNBMQswCQYDVQQIEwJCQzEQMA4GA1UEBxMHTmV3YnVyeTET
MBEGA1UECgwKUUFfU2FtcGx1MTESMBAGA1UECwwJU2FtcGx1X1FBMRwwGgYDVQQD
DBNzYW1wbGUxX3FhLnZpY3RvcmlhMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA6V6igVPc6bX3VDMXbxWcAFz/smTG5Ui+NqekVfSx38mBpEH+KYDW/dTE
tZe3wT1CbMD4Cc3qNvY7udnOFYctL7PyX/lCBuKgYlYGbcxlaWLbNjQJlVvD0OaF
7mR2Pu3WR7tJ8giBFMLjk9sguobnYCSAAX89t2AWugbUoeAY0XPKHiQVVm2XeYEE
9/03BkLXFYI0qlEszOLw0ULdtXG7EBmgClxPd7m7NpXtpHcH41D5NiAT4uF40go2
irk5kB+kghJPUCk/GX0WprMje7h7hWAEITmEHZ6B5SAsilHzUvc8T+bypYjcLpkK
s2UevzNfvtxTHKZpGMTHdb8g488prwIDAQABo2swaTAfBgNVHSMEGDAWgBR0SB68
8syKm4CUQ27LGB9ftHRZyTAMBgNVHRMBAf8EAjAAMA8GA1UdDwEB/wQFAwMHuAAw
JwYDVR0lBCAwHgYIKwYBBQUHAwQGCCsGAQUFBwMCBggrBgEFBQcDATALBgkqhkiG
9w0BAQUDggEBAJe1D1h623uD9mBjfB3YDKO3agm3vbdMd2vcdKI8TA5dsxMhmHvm
8E+gVsV0rNVbupLoc6OYeJLPvWQ54j9wZnKavBbma067C1QJJ2jEhOhjzo1EDIqT
l/qBhvqabhTG3vIMFSIwOu0zmQD/2iFu9cykKiru8A8djfZWjjfZiHO4dkkiCInP
/dor+Cm5RokGZ+OXhZ/5hxTuGeSAWJIhObVnrnPLZ2c2uYGh6LYip+2GU6L/rp8z
tmLYfldjtTMGYeP4Ivo1s7KHJqqDlAT0Bwe2XVR98O8SrHI7toSpAbdIqP+f77zv
pb5xvOSfmqLuV6eUvJW8d/Wj2mvgw1qLvqY=
-----END CERTIFICATE-----
```

Tenga este archivo a mano para copiar el contenido o para importarlo en el sistema Guardium.

cli> store certificate sniffer [console | import]

Si trabaja en la consola, copie y peque desde **-----BEGIN CERTIFICATE-----** hasta **-----END CERTIFICATE-----** (incluido todo lo de dentro de la copia) y péguelo en la cli cuando se le solicite. Si ha elegido importar, indique al sistema Guardium de dónde debe importar el archivo.

Se le solicitará que confirme que desea almacenar el certificado, y cuando lo confirme, se almacenará.

```
temp4 > store system certificate console
Please paste your new system certificate, in PEM format.
Include the BEGIN and END lines, then press CTRL-D.

-----BEGIN CERTIFICATE-----
MIID1jCCAscgAwIBAgIBCDALBgkqhkiG9w0BAQUwgYAxCzAJBgNVBAYTAkNBMRkw
FwYDVQQIExBCcml0aXNoIENvbHVtYmlhMREwDwYDVQQHEwhWaWN0b3JpYTEUMBIG
A1UEChMLUUFfdGVzdF92aWMxFDASBgNVBAsTC1ZpY3RvcmlhX1FBMRcwFQYDVQQD
Ew5WaWN0b3JpYV9RQV9DQTAeFw0xMDExMDEyMTA5MzhaFw0xNTExMDEyMTA5Mzha
MHMxCzAJBgNVBAYTAkNBMQswCQYDVQQIEwJCQzEQMA4GA1UEBxMHTmV3YnVyeTET
MBEGA1UECgwKUUFfU2FtcGxlMTESMBAGA1UECwwJU2FtcGxlX1FBMRwwGgYDVQQD
DBNzYW1wbGUxX3FhLnZpY3RvcmlhMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA6V6igVPc6bX3VDMXbxWcAFz/smTG5Ui+NqekVfSx38mBpEH+KYDW/dTE
tZe3wT1CbMD4Cc3qNvY7udnOFYctL7PyX/lCBuKgYlYGbcxlaWLbNjQJlvvD0OaF
7mR2Pu3WR7tJ8giBFMLjk9sguobnYCSAAX89t2AWugbUoeAYOXPKHiQVVm2XeYEE
9/03BkLXFYI0qlEszOLw0ULdtXG7EBmgClxPd7m7NpXtpHcH41D5NiAT4uF40go2
irk5kB+kghJPUCk/GX0WprMje7h7hWAEITmEHZ6B5SAsilHzUvc8T+bypYjcLpkK
s2UevzNfvtxTHKZpGMTHdb8g488prwIDAQABo2swaTAfBgNVHSMEGDAWgBR0SB68
8syKm4CUQ27LGB0ftHRZyTAMBgNVHRMBAf8EAjAAMA8GA1UdDwEB/wQFAwMHuAAw
JwYDVR0lBCAwHgYIKwYBBQUHAwQGCCsGAQUFBwMCBggrBgEFBQcDATALBgkqhkiG
9w0BAQUDggEBAJe1Dlh623uD9mBjfB3YDKO3agm3vbdMd2vcdKI8TA5dsxMhmHvm
8E+gVsVOrNVbupLoc6OYeJLPvWQ54j9wZnKavBbma067C1QJJ2jEhOhjzoiEDIqT
l/qBhvqabhTG3vIMFSIwOu0zmQD/2iFu9cykKiru8A8djfZWjjfZiHO4dkkiCInP
/dor+Cm5RokGZ+OXhZ/5hxTuGeSAWJIhObVnrnPLZ2c2uYGh6LYip+2GU6L/rp8z
tmLYfldjtTMGYeP4Ivo1s7KHJqqDlATOBwe2XVR98O8SrHI7toSpAbdIqP+f77zv
pb5xvOSfmqLuV6eUvJW8d/Wj2mvgw1qLvqY=
-----END CERTIFICATE-----
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8 (0x8)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CA, ST=British Columbia, L=Victoria, O=QA_test_vic, OU=Victori
a_QA, CN=Victoria_QA_CA
        Validity
            Not Before: Nov  1 21:09:38 2010 GMT
            Not After : Nov  1 21:09:38 2015 GMT
        Subject: C=CA, ST=BC, L=Newbury, O=QA_Sample1, OU=Sample_QA, CN=sample1_
qa.victoria
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:e9:5e:a2:81:53:dc:e9:b5:f7:54:33:17:6f:15:
                    9c:00:5c:ff:b2:64:c6:e5:48:be:36:a7:a4:55:f4:
                    b1:df:c9:81:a4:41:fe:29:80:d6:fd:d4:c4:b5:97:
                    b7:c1:3d:42:6c:c0:f8:09:cd:ea:36:f6:3b:b9:d0:
                    ce:15:87:2d:2f:b3:f2:5f:f9:42:06:e2:a0:62:56:
                    06:6d:cc:65:69:62:db:36:34:09:95:5b:c3:d0:e6:
                    85:ee:64:76:3e:ed:d6:47:bb:49:f2:08:81:14:c2:
                    e3:93:db:20:ba:86:e7:60:24:80:01:7f:3d:b7:60:
                    16:ba:06:d4:a1:e0:18:39:73:ca:1e:24:15:56:6d:
                    97:79:81:04:f7:fd:37:06:42:d7:15:82:34:aa:51:
                    2c:cc:e2:f0:d1:42:dd:b5:71:bb:10:19:a0:0a:5c:
                    4f:77:b9:bb:36:95:ed:a4:77:07:e3:50:f9:36:20:
                    13:e2:e1:78:d2:0a:36:8a:b9:39:90:1f:a4:82:12:
                    4f:50:29:3f:19:7d:16:a6:b3:23:7b:b8:7b:85:60:
                    04:21:39:84:1d:9e:81:e5:20:2c:8a:51:f3:52:f7:
                    3c:4f:e6:f2:a5:88:dc:2e:99:0a:b3:65:1e:bf:33:
                    5f:be:dc:53:1c:a6:69:18:c4:c7:75:bf:20:e3:cf:
                    29:af
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:74:48:1E:BC:F2:CC:8A:9B:80:94:43:6E:CB:18:1F:5F:B4:74:59:C
9

            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment, Data Encipherment, Key Agre
ement
            X509v3 Extended Key Usage:
                E-mail Protection, TLS Web Client Authentication, TLS Web Server
 Authentication
    Signature Algorithm: sha1WithRSAEncryption
        97:b5:0e:58:7a:db:7b:83:f6:60:63:7c:1d:d8:0c:a3:b7:6a:
        09:b7:bd:b7:4c:77:6b:dc:74:a2:3c:4c:0e:5d:b3:13:21:98:
        7b:e6:f0:4f:a0:56:c5:4e:ac:d5:5b:ba:92:e8:73:a3:98:78:
        92:cf:bd:64:39:e2:3f:70:66:72:9a:bc:16:e6:6b:4e:bb:0b:
        54:09:27:68:c4:84:e8:63:ce:88:84:0c:8a:93:97:fa:81:86:
        fa:9a:6e:14:c6:de:f2:0c:15:22:30:3a:ed:33:99:00:ff:da:
        21:6e:f5:cc:a4:2a:2a:ee:f0:0f:1d:8d:f6:56:8e:37:d9:88:
        73:b8:76:49:22:08:89:cf:fd:da:2b:f8:29:b9:46:89:06:67:
        e3:97:85:9f:f9:87:14:ee:19:e4:80:58:92:21:39:b5:67:ae:
        73:cb:67:67:36:b9:81:a1:e8:b6:22:a7:ed:86:53:a2:ff:ae:
        9f:33:b6:62:d8:7e:57:63:b5:33:06:61:e3:f8:22:fa:35:b3:
        b2:87:26:aa:83:94:04:ce:07:07:b6:5d:54:7d:f0:ef:12:ac:
        72:3b:b6:84:a9:01:b7:48:a8:ff:9f:ef:bc:ef:a5:be:71:bc:
        e4:9f:9a:a2:ee:57:a7:94:bc:95:bc:77:f5:a3:da:6b:e0:c3:
        5a:8b:be:a6

Do you want to store this certificate? (y/n)
```

Es necesario reiniciar el núcleo de inspección para que el nuevo certificado entre en vigor.

Instalación de un certificado generado fuera del sistema Guardium

Recibirá un par de archivos de la CA (además del certificado público para la CA) que es su certificado.

Una será el certificado público de la entidad emisora de certificados, como:

```
enance@enance1 Latest $ cat Victoria_QA_CA.pem
-----BEGIN CERTIFICATE-----
MIID2zCCAsWgAwIBAgIBATALBgkqhkiG9w0BAQUwgYAxCzAJBgNVBAYTAkNBMRkw
FwYDVQQIExBCcml0aXNoIENvbHVtYmlhMREwDwYDVQQHEwhWaWN0b3JpYTEUMBIG
A1UEChMLUUFfdGVzdF92aWMxFDASBgNVBAsTC1ZpY3RvcmlhX1FBMRcwFQYDVQQD
Ew5WaWN0b3JpYV9RQV9DQTAeFw0xMDA4MTIxODMzMDJaFw0zMDA4MTIxODMzMDJa
MIGAMQswCQYDVQQGEwJDQTEZMBcGA1UECBMQQnJpdGlzaCBDb2x1bWJpYTERMA8G
A1UEBxMIVmljdG9yaWExFDASBgNVBAoTC1FBX3R1c3RfdmljMRQwEgYDVQQLEwtW
aWN0b3JpYV9RQTEXMBUGA1UEAxMOVmljdG9yaWFfUUFfQ0EwggEgMAsGCSqGSIb3
DQEBAQOCAQ8AMIIBCgKCAQEA0x3iAXs1KGNoJThXkO+jcNyMBlfwKWRMTOq9PkF4
piznXCRwPz2nQWk5/fpslchmuVYXJtfZi7umDxp2FEMvMmhJfFZiqbCn1Rb5yH+1
V3RsIerB0DFpoWkdt+wD6BufndO5P9eOlv14bmTl+F0dUM0TxAwtX73CMQOX/n+i
/WrzpWU4lU71KkyWUfJl2Pm8TLEMr5awpzt2rEJ/Q1qItHcksQDbGY0MNLaNojEU
XBzUpu9ezbv+zVH+5iorFYkrH0NQI0NK+YoR1b3Tto0HLDh6istsMfHdNEEQb9BB
vMjqUz4tGB2HDguYTaNbQJj9Yw8uv7/tfwW/cesrqm8DiQIDAQABo2QwYjAPBgNV
HRMBAf8EBTADAQH/MA8GA1UdDwEB/wQFAwMHBgAwHQYDVR0OBBYEFHRIHrzyzIqb
gJRDbssYH1+0dFnJMB8GA1UdIwQYMBaAFHRIHrzyzIqbgJRDbssYH1+0dFnJMAsG
CSqGSIb3DQEBBQOCAQEAbrImEbRyBka0wO/ZuPd0Hw9jpbxIuaYEskakv7aM4TUQ
awf1CiqwwAymmKb2REItLajhjmBFbXBun7d137vBU2KX104I7WGw0xgI5rmlELa+
2fizugY+Bc6mh+5c0haizkyudKzo8mLz2p/IS7SPh2lJ9rnuBleSt9zfiYanPxX1
Q6z1+WRKIRSUmK+ho4bmtgr5F0+ejmZb9nfzeOBj23H9i0mWoaQ/SO+O2iDIvDY0
KYwqCeS2UNEdTcnfuczbBkqnAsf5/GBPIhnWX3onuLkOsHdY0HHPjoqgHauoxPK8
p0sEvlCK8EFOD6wkp0vtNhFQCykxRimHR6Pz9jEVjw==
-----END CERTIFICATE-----
```

Lo siguiente será el certificado público específico destinado a usted/este sistema Guardium, que tendrá este aspecto:

```
enance@enance1 Latest $ cat Sample_givenCert.victoria.qa_pub.pem
-----BEGIN CERTIFICATE-----
MIID5jCCAtCgAwIBAgIBCTALBgkqhkiG9w0BAQUwgYAxCzAJBgNVBAYTAkNBMRkw
FwYDVQQIExBCcml0aXNoIENvbHVtYmlhMREwDwYDVQQHEwhWaWN0b3JpYTEUMBIG
A1UEChMLUUFfdGVzdF92aWMxFDASBgNVBAsTC1ZpY3RvcmlhX1FBMRcwFQYDVQQD
Ew5WaWN0b3JpYV9RQV9DQTAeFw0xMDExMTUyMDUwNThaFw0xNTExMTUyMDUwNTha
MIGEMQswCQYDVQQGEwJDQTEZMBcGA1UECBMQQnJpdGlzaCBDb2xvbWJpYTESMBAG
A1UEBxMJVmFuY291dmVyMQswCQYDVQQKEwJRQTESMBAGA1UECxMJUUFfU0FNUExxF
MSUwIwYDVQQDExxTYW1wbGVfZ2l2ZW5DZXJ0LnZpY3RvcmlhLnFhMIIBIDALBgkq
hkiG9w0BAQEDggEPADCCAQoCggEBALdt2XhJEJIAognblgFNoiomVvcGIe9PHs0t
3fP5DxAL5PVm+UCRS0xnnCoKe3pdJNagepDwBa2K5UsHbK4vkHJEgWWEd4bx2Ks7
kRoHr83TXK+W8al1HGKRwUSwN0hfm/KV4v8ZX3AFWs2c/BJ2iA77a0mhU0JuWa1/
/scXitJB5ykPjFb2EuReA6ELphaQ/itjZIQTTeVxbamyx42ia9J5B07lFTp3qGdU
yXUwlEFX0HFPmknAAaQrSnpMdQjkOKgzxU0NTV4ILA66hCVkX+ezQeJA90s/AHA5
hAY2fyurKZsOowoE0xlEpFWCGf87zxfkmTaWthqCS0NzEcJ6efECAwEAAaNrMGkw
HwYDVR0jBBgwFoAUdEgevPLMipuAlENuyxgfX7R0WckwDAYDVR0TAQH/BAIwADAP
BgNVHQ8BAf8EBQMDB7gAMCcGA1UdJQQgMB4GCCsGAQUFBwMEBggrBgEFBQcDAgYI
KwYBBQUHAwEwCwYJKoZIhvcNAQEFA4IBAQB+P1m22B72eRESk9rgNdOB+l48k5xw
QHf64TJcoI/Vcz0vtGBC1jDfZzVDIHJaX6ZMtdO23QO6rtjQSnhjhbOt/EiimaNO
tysJOE999E+HQ7UpKYKvdoznwpYEthyoQJ9quKqQc1YW/l8pQMYDEdK8c7yMbJpv
mrxO8h+G3YYQMT6A9KAk/GPA+yKl0fCuogBhPyWM28q35EAIw6H9ahQigWhNkzrL
DCYO8VCLi3BX+OohLvurkyzJm2lnbm7BSb5QB4jISlRBGPoIWhK6VPypboyABfVs
yWHFVs10EUb0Maa/XNZILTAoYAbYK5sX7Ri5hr5KhxnmDd9AJMQsLfik
-----END CERTIFICATE-----
```

Lo último será una clave privada (cifrada con pkx#8) que se parecerá a la siguiente:

```
enance@enance1 Latest $ cat Sample_givenCert.victoria.qa_pri.pem
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIE4jAcBgoqhkiG9w0BDAEDMA4ECAKuMvSla9T4AgIBYgSCBMB/RzDgm4xpRDnA
Cd//wgD9c8junXmVpyJWXWgXhlj3Sgv3toKt2yBQY7Rv0peP1y68nuHKZcp/QZDj
QksDvIJHacpz886KQ2p9xxOCrIO3RTVNULPzrucUNuJ2a5W4IGPGwnrNLKsriRH6
CXQjRu19+kbczmPtrlHu7gj6MuCp58sIyXbsOPCnsZBaAOcf72qeKfVa4tKlpobI
e5YDg+UiJXYv1Kfj9t9tftSfaCym0jK+uE3++y5+ah/k+u/VcEb9b6DrlfG8KaJI
/OYVVmRWVIHEY2QjVOsVEXAARjpugf6cXIn8epw/CMaC0yVg4O9OGDrIz/41DVgk
/b3jlr1oWMRVASSqgOQxE2LrNNAF/XiFwpiLUCBHR0fXX9iKJM7nK6AXlf4hrd31
sMm1hICJvQwuRP+1xCHHs3qKk7oFAdyEdMiYthcOoAaynGmP4vPEMB6ZdOSxd/yN
7IfBT1U7nCtgo4FpAn4FTnkXRdlDqPpvKLqe0kkQCKo9ZWRnnIS1hAs9VJXS6zou
1IohZewrS/TWnPU+ArE/QJ4WkX2dBAe0Q2HMvuXs6J6Rfn+H2eZC+zThOkvqA0ic
UiQAgJB0ohXWEah9BJbIYNULLpbssUySDLPrxYdZRPn5MFKqCXmWw5tAEV8mIcg4
obB6DxVGHz93iPD0XJyBGWpCdcwItzdngnMR316tX4R3jMy2U0hrzk5o01GoZQQ/
eGYsuPzm4zqVJ8S9gUMFR8ocoPWqwhU+Sq4QPCIQEGf5gwxxt9j7L2TtRbD7kxnD
23aPL/wuk45EFJKTQCeZ3kjUqCCuSbqBJXGEjiiUsahus+yJULJ8boFWu1T8zW7m
/CBK1TzY9Fh+gbdOtN4b+zWUrpk5E7ZctFhEwojVFBwgPzUIZEkap4gH+/F5d3rI
uWFBcN7QER35wO8au/k5kLKHDh+5U15ltkJ38P1pJYFE0p5/K81YWnfvUaJmynJY
DfnK0X6Au69/F6+QR4S+bchbrqk73plIiXbkwqapQ26QH5ztIK3T6/nY6RKa7u6N
WvnskpAE1uxf+soM+BpEzpTl2gQQmEaZnh9Ci3ZnpTZE5tkAL0oTqXL9sToyeynz
Z91m+uKxYRjFvc1KPh+I8dUR0E5qXhBdRR7heIlm7/Dg+UqCUkXoyW89G14u/mJT
jB50CHxLAFOSeXnKn8G/9rOHA565r8L/z8D12sli5T1zHicZJ8O211zCSezdF+GG
mI12jf0ZmNIBgCVUtpOBNX5IDbr7L+0bM6vuDmXRhnhX4f34+5HGfj3ntLAV7bmn
IOEGIhyoGFnoxyWaT0xxa6MVQJazcKSyyyhO8UixFEoKI3drpFXB0tXVb0CLFq+y
QVp9dHgO3Otzw/yCmCpbQQe8UFRYyC74wBf9yPWDtN6MW/IeEZCBoYaeMR+WyonM
mdq5xbriETXD4zha3NGAv2qnzkfkKMBcVeUULulyixMsHmNNJkINNEsj5deVYtOt
4j5EK/aZsTqTgrVq3oGlwgXM1YptvlVR+HPWZfpjwbL+7/NhmK7AhEPo+qQCVD7t
ZGRbdbB7FEN23m88IMSd8xkhS2M1pop1Cj71P/dA+DD/dgcjP2bw7K923d4r3CcS
1yxPhLKM
-----END ENCRYPTED PRIVATE KEY-----
```

Tenga estos archivos a mano para importarlos (a través de scp/ftp/etc) en el sistema Guardium o para copiarlos y pegarlos en la interfaz de cli en el sistema Guardium.

Inicie una sesión en el sistema Guardium mediante la cli.

Para almacenar la clave privada:

cli> store certificate keystore [import | console]

la importación toma el archivo guardado, consola, y copia y pega el contenido del archivo en la interfaz de la consola.

Le solicitará la contraseña con la que se ha guardado el archivo. Es posible que la haya proporcionado a la CA para la creación del certificado, o, lo que es más probable, que se la hayan proporcionado con una contraseña cuando le enviaron los archivos.

Tiene este aspecto en el sistema Guardium:

```
temp4> store system key console
Please paste your new system key, in PEM format.
Include the BEGIN and END lines, then press CTRL-D.

-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIE4jAcBgoqhkiG9w0BDAEDMA4ECAKuMvSla9T4AgIBYgSCBMB/RzDgm4xpRDnA
Cd//wgD9c8junXmVpyJWXWgXhlj3Sgv3toKt2yBQY7Rv0peP1y68nuHKZcp/QZDj
QksDvIJHacpz886KQ2p9xxOCrIO3RTVNULPzrucUNuJ2a5W4IGPGwnrNLKsriRH6
CXQjRu19+kbczmPtrlHu7gj6MuCp58sIyXbsOPCnsZBaAOcf72qeKfVa4tKlpobI
e5YDg+UiJXYv1Kfj9t9tftSfaCym0jK+uE3++y5+ah/k+u/VcEb9b6DrlfG8KaJI
/OYVVmRWVIHEY2QjVOsVEXAARjpugf6cXIn8epw/CMaC0yVg4O9OGDrIz/41DVgk
/b3jlr1oWMRVASSqgOQxE2LrNNAF/XiFwpiLUCBHR0fXX9iKJM7nK6AXlf4hrd31
sMm1hICJvQwuRP+1xCHHs3qKk7oFAdyEdMiYthcOoAaynGmP4vPEMB6ZdOSxd/yN
7IfBT1U7nCtgo4FpAn4FTnkXRdlDqPpvKLqe0kkQCKo9ZWRnnIS1hAs9VJXS6zou
1IohZewrS/TWnPU+ArE/QJ4WkX2dBAe0Q2HMvuXs6J6Rfn+H2eZC+zTh0kvqA0ic
UiQAgJB0ohXWEah9BJbIYNULLpbssUySDLPrxYdZRPn5MFKqCXmWw5tAEV8mIcg4
obB6DxVGHz93iPD0XJyBGWpCdcwItzdngnMR316tX4R3jMy2U0hrzk5o01GoZQQ/
eGYsuPzm4zqVJ8S9gUMFR8ocoPWqwhU+Sq4QPCIQEGf5gwxxt9j7L2TtRbD7kxnD
23aPL/wuk45EFJKTQCeZ3kjUqCCuSbqBJXGEjiiUsahus+yJULJ8boFWu1T8zW7m
/CBK1TzY9Fh+gbd0tN4b+zWUrpk5E7ZctFhEwojVFBwgPzUIZEkap4gH+/F5d3rI
uWFBcN7QER35wO8au/k5kLKHDh+5U151tkJ38P1pJYFE0p5/K81YWnfvUaJmynJY
DfnK0X6Au69/F6+QR4S+bchbrqk73plIiXbkwqapQ26QH5ztIK3T6/nY6RKa7u6N
WvnskpAE1uxf+soM+BpEzpTl2gQQmEaZnh9Ci3ZnpTZE5tkAL0oTqXL9sToyeynz
Z91m+uKxYRjFvc1KPh+I8dUR0E5qXhBdRR7heIlm7/Dg+UqCUkXoyW89G14u/mJT
jB50CHxLAFOSeXnKn8G/9r0HA565r8L/z8D12sli5T1zHicZJ80211zCSezdF+GG
mI12jfOZmNIBgCVUtpOBNX5IDbr7L+0bM6vuDmXRhnhX4f34+5HGfj3ntLAV7bmn
IOEGIhyoGFnoxyWaT0xxa6MVQJazcKSyyyhO8UixFEoKI3drpFXB0tXVb0CLFq+y
QVp9dHgO3Otzw/yCmCpbQQe8UFRYyC74wBf9yPWDtN6MW/IeEZCBoYaeMR+WyonM
mdq5xbriETXD4zha3NGAv2qnzkfkKMBcVeUULulyixMsHmNNJkINNEsj5deVYtOt
4j5EK/aZsTqTgrVq3oGlwgXM1YptvlVR+HPWZfpjwbL+7/NhmK7AhEPo+qQCVD7t
ZGRbdbB7FEN23m88IMSd8xkhS2M1pop1Cj7lP/dA+DD/dgcjP2bw7K923d4r3CcS
1yxPhLKM
-----END ENCRYPTED PRIVATE KEY-----
Enter pass phrase for /var/tmp/key.pem:
writing RSA key

ok
temp4>
```

A continuación tiene que importar el certificado firmado con:

cli> store certificate sniffer [import | console]

Mostrará la información sobre el certificado y le pedirá que confirme que desea almacenar el certificado.

Tiene este aspecto:

```
temp4> store system certificate console
Please paste your new system certificate, in PEM format.
Include the BEGIN and END lines, then press CTRL-D.

-----BEGIN CERTIFICATE-----
MIID5jCCAtCgAwIBAgIBCTALBgkqhkiG9w0BAQUwgYAxCzAJBgNVBAYTAkNBMRkw
FwYDVQQIExBCcml0aXNoIENvbHVtYmlhMREwDwYDVQQHEwhWaWN0b3JpYTEUMBIG
A1UEChMLUUFfdGVzdF92aWMxFDASBgNVBAsTC1ZpY3RvcmlhX1FBMRcwFQYDVQQD
Ew5WaWN0b3JpYV9RQV9DQTAeFw0xMDExMTUyMDUwNThaFw0xNTExMTUyMDUwNTha
MIGEMQswCQYDVQQGEwJDQTEZMBcGA1UECBMQQnJpdGlzaCBDb2xvbWJpYTESMBAG
A1UEBxMJVmFuY291dmVyMQswCQYDVQQKEwJRQTESMBAGA1UECxMJUUFfU0FNUExF
MSUwIwYDVQQDExxTYW1wbGVfZ2l2ZW5DZXJ0LnZpY3RvcmlhLnFhMIIBIDALBgkq
hkiG9w0BAQEDggEPADCCAQoCggEBALdt2XhJEJIAognblgFNoiomVvcGIe9PHsOt
3fP5DxAL5PVm+UCRS0xnnCoKe3pdJNagepDwBa2K5UsHbK4vkHJEgWWEd4bx2Ks7
kRoHr83TXK+W8al1HGKRwUSwN0hfm/KV4v8ZX3AFWs2c/BJ2iA77a0mhU0JuWa1/
/scXitJB5ykPjFb2EuReA6ELphaQ/itjZIQTTeVxbamyx42ia9J5B07lFTp3qGdU
yXUwlEFX0HFPmknAAaQrSnpMdQjkOKgzxU0NTV4ILA66hCVkX+ezQeJA90s/AHA5
hAY2fyurKZsOowoE0xlEpFWCGf87zxfkmTaWthqCS0NzEcJ6efECAwEAAaNrMGkw
HwYDVR0jBBgwFoAUdEgevPLMipuAlENuyxgfX7R0WckwDAYDVR0TAQH/BAIwADAP
BgNVHQ8BAf8EBQMDB7gAMCcGA1UdJQQgMB4GCCsGAQUFBwMEBggrBgEFBQcDAgYI
KwYBBQUHAwEwCwYJKoZIhvcNAQEFA4IBAQB+Plm22B72eRESk9rgNdOB+l48k5xw
QHf64TJcoI/Vcz0vtGBC1jDfZzVDIHJaX6ZMtdO23QO6rtjQSnhjhbOt/EiimaNO
tysJOE999E+HQ7UpKYKvdoznwpYEthyoQJ9quKqQc1YW/l8pQMYDEdK8c7yMbJpv
mrxO8h+G3YYQMT6A9KAk/GPA+yKl0fCuogBhPyWM28q35EAIw6H9ahQigWhNkzrL
DCYO8VCLi3BX+OohLvurkyzJm2lnbm7BSb5QB4jISlRBGPoIWhK6VPypboyABfVs
yWHFVs10EUb0Maa/XNZILTAoYAbYK5sX7Ri5hr5KhxnmDd9AJMQsLfik
-----END CERTIFICATE-----
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 9 (0x9)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CA, ST=British Columbia, L=Victoria, O=QA_test_vic, OU=Victoria_QA, CN=Victoria_QA_CA
        Validity
            Not Before: Nov 15 20:50:58 2010 GMT
            Not After : Nov 15 20:50:58 2015 GMT
        Subject: C=CA, ST=British Colombia, L=Vancouver, O=QA, OU=QA_SAMPLE, CN=Sample_givenCert.victoria.qa
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:b7:6d:d9:78:49:10:92:00:a2:09:db:96:01:4d:
                    a2:2a:26:56:f7:06:21:ef:4f:1e:c3:ad:dd:f3:f9:
                    0f:10:0b:e4:f5:66:f9:40:91:4b:4c:67:9c:2a:0a:
                    7b:7a:5d:24:d6:a0:7a:90:f0:05:ad:8a:e5:4b:07:
                    6c:ae:2f:90:72:44:81:65:84:77:86:f1:d8:ab:3b:
                    01:1a:07:af:cd:d3:5c:af:96:f1:a9:75:1c:62:91:
                    c1:44:b0:37:48:5f:9b:f2:95:e2:ff:19:5f:70:05:
                    5a:cd:9c:fc:12:76:88:0e:fb:6b:49:a1:53:42:6e:
                    59:ad:7f:fe:c7:17:8a:d2:41:e7:29:0f:8c:56:f6:
                    12:e4:5e:03:a1:0b:a6:16:90:fe:2b:63:64:84:13:
                    4d:e5:71:6d:a9:b2:c7:8d:a2:6b:d2:79:07:4e:e5:
                    15:3a:77:a8:67:54:c9:75:30:94:41:57:d0:71:4f:
                    9a:49:c0:01:a4:2b:4a:7a:4c:75:08:e4:38:a8:33:
                    c5:4d:0d:4d:5e:08:2c:0e:ba:84:25:64:5f:e7:b3:
                    41:e2:40:f7:4b:3f:00:70:39:84:06:36:7f:2b:ab:
                    29:9b:0e:a3:0a:04:d3:19:44:a4:55:82:19:ff:3b:
                    cf:17:e4:99:36:96:b6:1a:82:4b:43:73:11:c2:7a:
                    79:f1
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:74:48:1E:BC:F2:CC:8A:9B:80:94:43:6E:CB:18:1F:5F:B4:74:59:C9

            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
            X509v3 Extended Key Usage:
                E-mail Protection, TLS Web Client Authentication, TLS Web Server Authentication
    Signature Algorithm: sha1WithRSAEncryption
        7e:3e:59:b6:d8:1e:f6:79:11:12:93:da:e0:35:d3:81:fa:5e:
        3c:93:9c:70:40:77:fa:e1:32:5c:a0:8f:d5:73:3d:2f:b4:60:
        42:d6:30:df:67:35:43:20:72:5a:5f:a6:4c:b5:d3:b6:dd:03:
        ba:ae:d8:d0:4a:78:63:85:b3:ad:fc:48:a2:99:a3:4e:b7:2b:
        09:38:4f:7d:f4:4f:87:43:b5:29:29:82:af:76:8c:e7:c2:96:
        04:b6:1c:a8:40:9f:6a:b8:aa:90:73:56:16:fe:5f:29:40:c6:
        03:11:d2:bc:73:bc:8c:6c:9a:6f:9a:bc:4e:f2:1f:86:dd:86:
        10:31:3e:80:f4:a0:24:fc:63:c0:fb:22:a5:d1:f0:ae:a2:00:
        61:3f:25:8c:db:ca:b7:e4:40:08:c3:a1:fd:6a:14:22:81:68:
        4d:93:3a:cb:0c:26:0e:f1:50:8b:8b:70:57:f8:ea:21:2e:fb:
        ab:93:2c:c9:9b:69:67:6e:6e:c1:49:be:50:07:88:c8:4a:54:
        41:18:fa:08:5a:12:ba:54:fc:a9:6e:8c:80:05:f5:6c:c9:61:
        c5:56:cd:74:11:46:f4:31:a6:bf:5c:d6:48:2d:30:28:60:06:
        d8:2b:9b:17:ed:18:b9:86:be:4a:87:19:e6:0d:df:40:24:c4:
        2c:2d:f8:a4

Do you want to store this certificate? (y/n)
y
ok
temp4>
```

Es necesario reiniciar el núcleo de inspección para que el nuevo certificado entre en vigor.

Configuración de S-TAP para que utilice la autenticación de certificado x.509

En primer lugar, tome nota de lo que ha asignado como CA y CN del certificado. Si no lo recuerda, utilice el mandato de cli show system certificate para ver los valores.

```
temp4 > show system certificate
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8 (0x8)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CA, ST=British Columbia, L=Victoria, O=QA_test_vic, OU=Victoria_QA, CN=Victoria_QA_CA
        Validity
            Not Before: Nov  1 21:09:38 2010 GMT
            Not After : Nov  1 21:09:38 2015 GMT
        Subject: C=CA, ST=BC, L=Newbury, O=QA_Sample1, OU=Sample_QA, CN=sample1_qa.victoria
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
```

Necesita el CN del certificado instalado en el sistema Guardium y la clave pública para la entidad emisora de certificados que ha firmado el certificado en el sistema Guardium. También es posible que desee una lista de revocación de certificados firmada por la misma entidad emisora de certificados que ha firmado el certificado del sistema Guardium, aunque no es necesario.

Los parámetros del archivo guard_tap.ini que le interesan son los mismos en Unix y en Windows:

```
; Where is the CA certificate
guardium_ca_path=NULL
; What's the CN to expect from the SqlGuard certificate?
sqlguard_cert_cn=NULL
; Path to crls file or dir
guardium_crl_path=NULL
```

La única diferencia funcional entre UNIX y Windows es que, en Windows, si no elige utilizar un valor para un parámetro, simplemente no lo incluya en el archivo guard_tap.ini, en lugar de asignarle el valor NULL. (Esto se aplica a la vía de acceso de CRL en particular, o si desea cerrar la autenticación de certificado y volver a TLS).

Copie la clave pública (y CRL si lo desea) de la CA que la CA le ha enviado en un directorio del host S-TAP. Tome nota de este directorio.

Establezca guardium_ca_path=[path-to-CA.pem]

Establezca sqlguard_cert_cn=[CN completo o CN parcial (utilizando * como carácter comodín) del sistema Guardium]

Establezca guardium_crl_path=[path-to-crl.crl] <-- solo si desea utilizar una lista de revocación de certificados en este momento.

En la vida real, tendría este aspecto:

```
guardium_ca_path=/var/tmp/pki/Victoria_QA_CA.pem
sqlguard_cert_cn=sample1_qa.victoria
guardium_crl_path=/var/tmp/pki/Victoria_QA_CA.crl
```

Una vez establecidos estos parámetros, cambie tls=1 y reinicie el S-TAP.

Ahora estará conectado mediante Openssl.

Tema principal: S-TAPs y otros agentes

Aumento del rendimiento de S-TAP

Puede configurar un S-TAP que notifique a varios sistemas Guardium para aumentar el rendimiento de los datos.

Puede configurar cualquier S-TAP para crear varias hebras a fin de aumentar el rendimiento de los datos. Si el archivo de configuración de S-TAP define más de un sistema Guardium, se puede crear una hebra para cada sistema Guardium. S-TAP crea hebras adicionales, cuyo número coincide con el número de sistemas de Guardium, en v10.1.4 y superior hasta un máximo de 10 hebras. Cuando el parámetro participate_in_load_balancing se establece en 4, el K-TAP crea un número similar de almacenamientos intermedios que coincide con el número de sistemas de Guardium hasta un máximo de 5 hebras. K-TAP va alternando entre almacenamientos intermedios, colocando en cada almacenamiento intermedio paquetes enteros. Cada hebra de S-TAP lee desde un almacenamiento intermedio de K-TAP diferente y envía datos sobre el tráfico a un único sistema Guardium.

En esta configuración, ningún Guardium recibe todos los datos del S-TAP. La distribución es parecida a la que se utiliza cuando participate_in_load_balancing está establecido en 1.
Atención: Antes de la V10 GPU200, cuando un sistema Guardium dejaba de estar disponible, no se proporciona ningún método de sustitución por anomalía. Los datos que se estaban enviando a un sistema Guardium se perdían hasta que el sistema volvía a estar disponible o hasta que se cambiaba la configuración.
Atención: Con anterioridad a la V10 GPU300, si el archivo de configuración de S-TAP definía más de un sistema de Guardium, se podía crear una hebra para cada sistema Guardium. Esta característica se activa solo cuando el parámetro participate_in_load_balancing se establece en 4.

El tráfico de A-TAP cifrado y sin cifrar no se puede enviar al mismo sistema Guardium. Esta situación es parecida a la que se produce cuando participate_in_load_balancing se establece en 1

Tema principal: S-TAPs y otros agentes

S-TAP de UNIX

Instalación y configuración de S-TAP de UNIX.

Un S-TAP de UNIX es un daemon de espacio de usuario que recopila datos de diversas fuentes para enviarlos al sistema Guardium para su análisis y registro. Recopila tráfico de: KTAP - módulo del kernel que realiza la interceptación en el kernel; ATAP - bibliotecas de espacio de usuario que se cargan cuando una base de datos empieza a recopilar tráfico; y bibliotecas EXIT para enviar el tráfico directamente del servidor de base de datos a S-TAP.

Cambios en la v10.1.4 a S-TAP de UNIX

- Directorio de subida dedicado para subir módulos y diagnósticos desde el servidor de bases de datos:
  - Instalación de shell – guardium/guard_stap/.upload
  - Instalación de GIM – modules/STAP/current/.upload
- ATAP generará un aviso en el registro de S-TAP para procesos que no pertenezcan al grupo adecuado cuando se abre la sesión.
- Cambios a guardctl
  - save-active-ataps - Guarda la configuración de cada ATAP activado actualmente en etc/guard/saved_ataps
  - restore-saved-ataps - Restaura los ATAP guardados en etc/guard/saved_ataps en el estado activo y almacenado
  - El mandato de reparación se ejecuta de forma automática durante la activación y desactivación cuando guardctl detecta que es necesario hacerlo.
- guard-config-update ahora da soporte a entornos GIM y a más opciones.
- Cambios a guard_monitor
  - La medición de CPU es configurable para que se base en todo el sistema o por procesador individual (cpu_measurement_mode)
  - El limpiador utiliza casos para la generación de núcleo forzada (force_core_when)

Novedades o mejoras de la V10

STAP de 64 bits

- El binario de S-TAP para plataformas de 64 bits ahora se compila como binario de 64 bits
- Aumenta la cantidad de datos que S-TAP puede correlacionar para el almacenamiento intermedio
- Entero de 32 bits con signo máximo - aproximadamente 2Gb (asignados por sqlguard_ip)

Claves de sesión de 64 bits

- Reduce la probabilidad de colisiones de clave que generan pérdidas de tráfico
- El efecto colateral es que un S-TAP de la V-10 sólo se puede conectar a un sistema Guardium V10

Veredicto rápido de SHMEM

- Activado de forma predeterminada
- Para un veredicto rápido de SHMEM, utilice el nombre de parámetro ktap_fast_shmem.

- Transmite la información necesaria sobre DB2 al kernel para determinar si el segmento pertenece a la base de datos
- La configuración del motor de inspección no se modificado
- Transmite db2_shmem_size, db2_shmem_client_position y db2_fix_pack_adjustment, así como dev/ino del ejecutable en db_exec_file
- Puede resultar difícil de depurar, por lo que recomiende inhabilitarlo si se tienen problemas para interceptar el tráfico de SHMEM
- KTAP Informix se ha mejorado para capturar tráfico y eliminar limitaciones en segmentos

Veredicto rápido de TCP predeterminado

- Activado de forma predeterminada
- Los parámetros Network/Exclude_Network reciben soporte para el veredicto rápido
- Se da soporte a un máximo de 20 motores de inspección con un máximo de 20 entradas en cada Network/Exclude_Network, después de lo que se degrada a fast_verdict off - Si fast_tcp_verdict está activado y hay más del máximo de 20 soportados {motores de inspección, máscaras de red, exclusión de máscaras de red) configurados para interceptar el tráfico de TCP, fast_tcp_verdict se inhabilitará.

Nota: Debido a la complejidad y diversidad de entornos, hay notas que, si no se leen detenidamente y se siguen, pueden hacer que las instalaciones/actualizaciones fallen o funcionen incorrectamente. Aunque no todas están incluidas, para facilitar la búsqueda de estas notas, se muestran las secciones siguientes para ayudar al lector a identificar las áreas que requieren especial atención.

- Actualización de K-TAP dinámica frente a no dinámica (Solaris, AIX, HP-UX)
- Cadenas de UID (zonas de Solaris, WPAR de AIX, Solaris 8/9, Solaris 11 SPARC)
- Antes de instalar S-TAP en un host UNIX (zonas de Solaris)
- Mantenga UNIX S-TAP con GIM (IBM® DB2 pureScale)
- Instale UNIX S-TAP (Linux, AIX)
- Actualice el programa de utilidad del procedimiento (SUSE 11, HP-UX)
- Elimine el S-TAP de UNIX anterior (manual) (HP-UX, AIX WPAR)

Cómo inicializan los procesos S-TAP/GIM los distintos tipos y versiones de SO

Tabla 1. Procesos iniciales de S-TAP y GIM por parte de distintos SO

SO	Versión		Método de inicialización
AIX	6.1	PowerPC	inittab
AIX	7.1	PowerPC	inittab
AIX	7.2	PowerPC	inittab
HP-UX	11.11	pa9000	inittab
HP-UX	11.23	IA-64	inittab
HP-UX	11.23	pa9000	inittab
HP-UX	11.31	IA-64	inittab
HP-UX	11.31	pa9000	inittab
RHEL	4	i686	inittab
RHEL	4	IA-64	inittab
RHEL	4	x86_64	inittab
RHEL	5	i686	inittab
RHEL	5	IA-64	inittab
RHEL	5	ppc64	inittab
RHEL	5	s390x	inittab
RHEL	5	x86_64	inittab
RHEL	6	i686	inittab
RHEL	6	ppc64	inittab
RHEL	6	s390x	inittab
RHEL	6	x86_64	inittab
RHEL	7	ppc64le	systemd
RHEL	7	ppc64	systemd
RHEL	7	s390x	systemd
RHEL	7	x86_64	systemd
SUSE	11	i686	inittab
SUSE	11	ppc64	inittab
SUSE	11	s390x	inittab
SUSE	11	x86_64	inittab
SUSE	12	ppc64le	systemd
SUSE	12	s390x	systemd

SO	Versión		Método de inicialización
SUSE	12	x86_64	systemd
Ubuntu	10.04	x86_64	inittab
Ubuntu	12.04	x86_64	upstart
Ubuntu	14.04	x86_64	upstart
Ubuntu	16.04	x86_64	systemd
Solaris	5.10	i386	service
Solaris	5.10	i386_64	service
Solaris	5.10	SPARC	service
Solaris	5.11	i386_64	service
Solaris	5.11	SPARC	service

Esta es una tabla genérica para todas las versiones de Guardium. Consulte el documento sobre plataformas soportadas y requisitos previos para verificar si la plataforma específica recibe soporte para su versión de Guardium.

Notas

Servidores Upstart

Cuando se utilizan servidores Upstart, estos son los mandatos start y stop en el servidor de base de datos:

Para detener el proceso de S-TAP:

stop utap

Para iniciar el proceso de S-TAP:

start utap

Para detener los procesos de GIM y del supervisor:

stop gim_revision#

stop gsvr_revision#

Ejemplo, stop gim_46743

Para iniciar los procesos de GIM y del supervisor:

start gim_revision#

start gsvr_revision#

Ejemplo: start gim_46743

Para verificar el estado del producto Guardium en el sistema:

initctl list

status utap

Servidores systemd

Cuando se utilizan servidores systemd, estos son los mandatos en el servidor de base de datos:

Para detener el proceso de S-TAP:

systemctl stop guard_utap.service

Para iniciar el proceso de S-TAP:

systemctl start guard_utap.service

Para detener los procesos de GIM y del supervisor:

systemctl stop guard_gim.service

systemctl stop guard_gsvr.service

Para iniciar los procesos de GIM y del supervisor:

systemctl start guard_gim.service

systemctl start guard_gsvr.service

Para verificar el estado del producto Guardium en el sistema:

systemctl -t service -a|grep guard

Servidores de servicios

Cuando se utilizan servidores de servicios, estos son los mandatos en el servidor de base de datos:

Para detener el proceso de S-TAP:

svcadm -v disable guard_utap

Para iniciar el proceso de S-TAP:

svcadm –v enable guard_utap

Para detener los procesos de GIM y del supervisor:

svcadm –v disable guard_gim

svcadm –v disable guard_gsvr

Para iniciar los procesos de GIM y del supervisor:

svcadm –v enable guard_gim

svcadm –v enable guard_gsvr

Para verificar el estado del producto Guardium en el servidor:

svcs | grep guard

Referencia

Si ejecuta S-TAP en RHEL 7, consulte Flash Alert: http://www.ibm.com/support/docview.wss?uid=swg21977093

Requisitos del sistema de Guardium V10.0 (plataformas soportadas) (octubre de 2015)

64 bits

http://www-01.ibm.com/support/docview.wss?uid=swg27045976

Requisitos del sistema para V9.5 (plataformas soportadas) (marzo de 2015)

32 bits y 64 bits

http://www-01.ibm.com/support/docview.wss?&uid=swg27045286

La instalación y operación de la base de datos falla si se ha configurado RemoveIPC=yes para systemd

En RedHat Enterprise Linux 7, init se ha sustituido por systemd, que intenta limpiar IPC después de usuario que no sean del sistema después de que se salga del proceso. Esto ocasiona problemas con DB2 y Discovery al suprimirse los segmentos de memoria compartida de DB2. Para solucionar este problema, emita "RemoveIPC=no" en /etc/systemd/logind.conf y reinicie el sistema. Oracle también ha documentado que se necesita este valor para el funcionamiento correcto de la base de datos. Busque "La instalación y operación de la base de datos falla si se ha configurado RemoveIPC=yes para systemd".

Soporte de cifrado SSL de Sybase 15

La interceptación de tráfico cifrado SSL para Sybase 15 recibe soporte en las plataformas siguientes:

- Linux: todas las distribuciones y versiones soportadas
- Solaris 8, 9, 10 (solo SPARC)
- AIX 5.3 (con el parche LDR_PRELOAD)
- HPUX 11.00, 11.11, 11.23 y 11.31 (solo PARISC)

Se da soporte a los métodos de invocación guardctl y basado en la GUI. Si se utiliza el método basado en la GUI, el usuario del sistema operativo Sybase se debe añadir al grupo de Guardium antes de la invocación. En la definición del motor de inspección de Sybase, se debe especificar el parámetro de vía de acceso del ejecutable de BD (db_exec_path en guard_tap.ini) y debe contener la vía de acceso completa al ejecutable de Sybase (dataserv).

Secuencia del cargador de KTAP para la instalación del S-TAP de Linux de Guardium

El mecanismo del cargador de KTAP utiliza la secuencia siguiente para la instalación del S-TAP de Linux (con GIM y no GIM).

Nota: El mecanismo del cargador de KTAP continuará automáticamente con el paso siguiente si el paso anterior no se ha realizado correctamente.

1. El cargador de KTAP encuentra una coincidencia exacta de módulo de kernel para el nivel de sistema operativo y lo carga.
2. El cargador de KTAP comprueba si hay un módulo de kernel compatible probado en la lista de archivos ktap-combos.txt (KTAP_List_of_Modules) y los carga.
3. El cargador de KTAP compila el módulo KTAP localmente y lo carga. KTAP sólo se compilará en el sistema si el sistema tiene instalados los paquetes necesarios (gcc y kernel-devel para el kernel arrancado).
4. Si el mecanismo FlexLoad está activado, el cargador de KTAP buscará el módulo de kernel más cercano y lo cargará.

   Para activar el mecanismo FlexLoad, utilice los distintivos siguientes:

   Para una instalación de shell, utilice la opción: "--ktap_allow_module_combos"

   Para una instalación de GIM, utilice la opción: "KTAP_ALLOW_MODULE_COMBOS=Y"
5. El cargador de KTAP genera el mensaje "No se ha podido cargar" e instala el S-TAP sin el KTAP (o la instalación de S-TAP falla)

Nota: Consulte la información sobre lotes personalizados en el tema sobre los parámetros de KTAP.

Mecanismos de supervisión de S-TAP de UNIX

En función de cómo esté instalado y configurado, el S-TAP de UNIX recopila el tráfico utilizando diversos mecanismos. Independientemente del mecanismo utilizado, el tráfico se filtra, de modo que sólo se recopila el tráfico relacionado con la base de datos para conjuntos específicos de direcciones IP de cliente y servidor.

K-TAP

K-TAP es un módulo de kernel que está instalado en el sistema operativo. Una vez instalado, se puede habilitar o inhabilitar utilizando un valor del archivo de configuración. Cuando está habilitado, observa el acceso a un servidor de base de datos mediante un enganche con los mecanismos utilizados para la comunicación entre el servidor y el cliente de base de datos. Cuando K-TAP está inhabilitado, se puede utilizar Tee para supervisar el tráfico local. K-TAP y Tee son casi siempre mutuamente excluyentes: para supervisar el acceso local, puede utilizar K-TAP o Tee. Con K-TAP no es necesario cambiar la forma en que los clientes de base de datos se conectan al servidor.

En el momento de la instalación, elegirá si desea o no cargar el módulo kernel de K-TAP en el sistema operativo del servidor. Esta es la única manera de cargar dicho módulo. Si inicialmente no carga K-TAP y más adelante decide que desea utilizarlo, tendrá que eliminar S-TAP y luego volver a instalarlo.
Nota: Si K-TAP no se puede cargar correctamente durante la instalación, posiblemente debido a un problema de compatibilidad de hardware o software, Tee se instala como mecanismo de recopilación predeterminado. Para volver a utilizar K-TAP, después de que se hayan resuelto los problemas de compatibilidad, siga los pasos descritos en el apartado sobre conmutación de Tee a K-TAP.
Nota: El tráfico interno de la sesión se transfiere del KTAP antiguo al nuevo KTAP mediante una devolución de llamada. Esto significa que, para la mayoría de las bases de datos, pueden ser necesarias dos solicitudes de SQL antes de que se reanude la interceptación con el nuevo KTAP para las sesiones preexistentes. En el caso de Sybase IOCP, se necesitan tres solicitudes de SQL debido a la naturaleza de la sesión.

A-TAP

Un mecanismo de A-TAP (TAP a nivel de aplicación) supervisa la comunicación entre los componentes internos del servidor de base de datos. Se utiliza para el tráfico que solo se puede inspeccionar a nivel de aplicación de servidor de bases de datos, por ejemplo porque el DBMS utiliza su propio cifrado, o debido a otros detalles de implementación internos de la base de datos. A-TAP utiliza K-TAP como proxy para pasar datos a S-TAP, y se debe configurar por separado para cada instancia de base de datos que se deba supervisar.

A-TAP se utiliza para supervisar estos tipos de tráfico:

- Tráfico cifrado ASO para Oracle (versiones 9, 10, 11, 12c) en AIX, HPUX, Solaris y Linux
- Tráfico cifrado SSL para Oracle (versiones 10,11, 12c) en Linux, AIX, Solaris y HPUX (plataformas que dan soporte a LD_PRELOAD)
- Tráfico cifrado SSL para Sybase (versión 15) en AIX (solo AIX 5.3 con el parche LDR_PRELOAD o más reciente), Solaris (SPARC) y Linux (32 bits).
- Tráfico de memoria compartida para DB2 y Informix en Linux

PCAP

PCAP es un mecanismo de captura de paquetes que está a la escucha el tráfico de red procedente de un servidor de base de datos y destinado al mismo. En un entorno UNIX, puesto que K-TAP captura todo el tráfico de red, PCAP raramente se utiliza. En un entorno Windows, se utiliza PCAP para capturar el tráfico de red no cifrado (excepto para IA64). Además, en Linux, se utiliza PCAP para capturar el tráfico TCP/IP local en el dispositivo.

Para utilizar PCAP en un entorno de zonas de Solaris, debe añadir las direcciones IP de todas las zonas que desee supervisar al parámetro alternate_ips en el archivo guard_tap.ini de la máquina Solaris.

Consejo: El PCAP utiliza los valores de IP/máscara de cliente para todos los motores de inspección locales a fin de determinar lo se debe supervisar y notificar. Si el PCAP está instalado con un S-TAP con varios motores de inspección, y dichos motores tienen distintos valores de IP/máscara de cliente, el PCAP captura el tráfico procedente de todos los clientes que están definidos en todos los motores de inspección. Esto puede dar como resultado que se procese y se envíe más información al sistema Guardium de la que se pretendía.

Tee

Tee es un mecanismo de proxy que lee y reenvía el tráfico de los clientes locales a un servidor de base de datos. Cuando Tee recibe tráfico de base de datos, reenvía una copia al servidor de base de datos y una copia a S-TAP. Cuando se utiliza Tee, los clientes de base de datos deben conectarse al puerto de escucha de Tee en lugar de al puerto de escucha de la base de datos. Esto significa que debe modificar el modo en que el cliente de base de datos se conecta al servidor, o el modo en que el servidor de base de datos acepta las conexiones de cliente. En cualquier caso, normalmente se trata de un cambio de configuración menor en uno o dos archivos (en función del tipo de base de datos) y el resultado final es que, en lo que respecta a los clientes, Tee es la base de datos y, en lo que se refiere a la base de datos, Tee es el cliente. Todo este proceso es transparente tanto para los clientes como para el servidor, pero el cambio de configuración es necesario para garantizar que la conexión se realiza a través de Tee. Cuando se utiliza Tee, los clientes de base de datos pueden omitir Tee conectándose al puerto de escucha de la base de datos (en lugar de al puerto de escucha de Tee) o utilizando conductos con nombre, memoria compartida u otros mecanismos de conexión entre procesos en función del tipo de base de datos. Para obtener información detallada sobre cómo configurar los clientes para que se conecten a Tee, consulte el tema sobre la preparación de los clientes locales para que utilicen Tee.

Llamamos conexiones inesperadas a las conexiones que no se realizan a través del puerto de escucha de Tee. Cuando se utiliza Tee, puede habilitar un componente opcional denominado Hunter para observar, informar y, opcionalmente, inhabilitar las conexiones inesperadas. Hunter se ejecuta a intervalos aleatorios, por lo que es posible que no detecte todas estas conexiones y, aunque puede informar sobre conexiones inesperadas y, opcionalmente, inhabilitarlas, no puede auditar las acciones que han realizado dichas conexiones. Otro aspecto de Hunter es que cuando se activa para que detecte conexiones inesperadas, puede hacer un uso intensivo de la CPU, por lo que, si observa el proceso Hunter en ese momento, puede parecer que está consumiendo una gran cantidad de recursos de CPU del servidor. (El uso de la CPU disminuirá rápidamente después de un pico momentáneo).
Nota: Para utilizar Hunter, debe tener instalada la versión 5.8.0 o posterior de Perl en el directorio /usr/bin/.
Nota: Sólo en Solaris 11 - Si no se ha instalado inicialmente Tee, es necesario realizar una reinstalación. O bien TEE se debe instalar manualmente.

Actualizaciones de K-TAP - dinámica frente a no dinámica

Las actualizaciones de K-TAP dan soporte a una actualización dinámica y sin reinicio mediante el uso del parámetro obligatorio KTAP_LIVE_UPDATE. Este parámetro se debe establecer durante cada actualización y se controla a través de los instaladores de GUI o BUNDLE-STAP/KTAP.

- Antes de ejecutar una actualización dinámica, ya sea a través de instaladores de GIM o de shell, debe asegurarse de que ningún proceso esté utilizando el dispositivo K-TAP. S-TAP debe estar detenido y A-Tap debe estar desactivado. Ejecute fuser /dev/ktap_xxx o lsof | grep ktap_xxx (donde xxx es el número de versión anterior) para ver si algún proceso está manteniendo abierto el dispositivo. Si no lo hace, puede experimentar un comportamiento imprevisible.
- Desde la GUI, el nuevo parámetro de K-TAP KTAP_LIVE_UPDATE se inicializará (en blanco) cada vez que se desee actualizar. Al igual que cualquier otro parámetro obligatorio no inicializado, el parámetro se debe establecer antes de continuar con el proceso de actualización.
  Los valores válidos para el parámetro nuevo son:
  - Y/y – Para una actualización de K-TAP dinámica (sin reinicio)
  - N/n – Para una actualización de K-TAP no dinámica (es necesario reiniciar el sistema para completar la actualización)
- Cuando se actualiza K-TAP mediante KTAP/BUNDLE-STAP, la instalación se realiza directamente en el servidor de BD. La nueva característica impondrá la especificación de un argumento nuevo en la línea de mandatos donde el nombre de argumento es -- live_update [Y|N].

- Después de una actualización dinámica de K-TAP:
  - El primer SQL para una sesión existente después de actualizar K-TAP no se capturará.
  - La sesión de ATAP existente en la zona local de Solaris no se registrará.
  - Es posible que algunos procesos sigan haciendo referencia a la memoria del módulo de K-TAP antiguo. En este escenario, el módulo rechaza liberar los recursos para evitar una futura inestabilidad. Cuando esto sucede, el usuario debe, después de que estos recursos ya no se utilicen, intentar una limpieza manual ejecutando el mandato guard_ktap_cleanup que se encuentra en el directorio ktap.
  - En HP-UX 11.11, el módulo de K-TAP antiguo ya no se instalará, pero seguirá apareciendo como registrado cuando se ejecute kmadmin -s | grep tap. El registro del módulo se debe eliminar manualmente con kmmodreg -U ktap_<versión>.
  - En Solaris y AIX, los nodos de dispositivo antiguos no se suprimirán automáticamente después de un rearranque y se tendrán que eliminar manualmente.

Excepciones:

- Si el servidor de base de datos está instalado con una versión que no se ha instalado mediante GIM, y la versión de K-TAP que no es de GIM no es la misma con la instalación de la versión de K-TAP, el valor de KTAP_LIVE_UPDATE se pasará por alto, ya que una actualización desde una versión que no es de GIM requiere un rearranque del sistema
- En una instalación desde cero, el valor KTAP_LIVE_UPDATE se pasará por alto
- Si el sistema se actualiza desde una versión que no es de GIM a la misma versión de GIM, no es necesario rearrancar el sistema
- NO puede volver a instalar una versión de K-Tap instalada anteriormente sin reiniciar la máquina

Manejo de errores:

- En el caso de que se produzca un error, es extremadamente importante comprobar el informe Lista de sucesos de GIM, ya que algunos errores requerirán un rearranque del sistema para poder recuperarse totalmente.

Nota: Sólo K-TAP para AIX no se podrá cargar durante una instalación o actualización de S-TAP si no se ha definido el entorno de ODMDIR. ODMDIR corresponde a Object Data Manager Directory. ODM es una base de datos de información de configuración de dispositivos y sistemas integrada en el sistema operativo. Está diseñada para almacenar información del sistema, información de software e información de dispositivos. Todos los mandatos de ODM utilizan la variable de entorno ODMDIR, que se establece en el archivo /etc/environment. El valor predeterminado de ODMDIR es /etc/objrepos.

Discovery Agent

Guardium Discovery Agent es un agente de software que se instala automáticamente con el paquete de S-TAP en un sistema servidor de base de datos. Su finalidad es la de detectar las instancias de base de datos que se ejecutan en el servidor de base de datos y notificarlas al sistema Guardium. Para que Discovery Agent funcione, todas las bases de datos del servidor de base de datos que desea descubrir deben estar iniciada.

Nota: En la arquitectura de zonas de Solaris, cuando las instancias de DB2 se ejecutan en zonas esclavas, el descubrimiento no descubrirá los parámetros de memoria compartida de DB2.

Las bases de datos recién descubiertas se pueden ver en el informe de instancias descubiertas. Los orígenes de datos y los motores de inspección se pueden añadir rápidamente a este informe mediante las herramientas de generación de entrada de GuardAPI.

Si las bases de datos del servidor de base de datos no están operativas (iniciadas) o se añadirán más tarde, Discovery Agent puede seguir descubriendo estas instancias si Discovery Agent ha realizado el ciclo (se ha inhabilitado y luego habilitado) en ese servidor de base de datos. Consulte Interfaces de usuario de GIM para obtener más información sobre cómo modificar los parámetros de los módulos instalados. Para Discovery Agent se debería cambiar el parámetro discovery_enabled por 2-inhabilitado y luego de nuevo por 1-habilitado para que realice un ciclo correcto.
Nota: Discovery Agent notifica sus hallazgos al S-TAP de destino primario, NO al sistema que aparece como GIM_URL o S-TAP de destino secundario.

Mantenimiento del S-TAP de Unix con GIM

Las funciones de instalación automática y simplificada de Guardium Installation Manager (GIM) lo convierten en el método de instalación principal para los módulos de Guardium como S-TAP y CAS en un entorno Unix. Después de una instalación sencilla guiada por un asistente de un cliente GIM en el servidor de base de datos, la instalación de los módulos se puede planificar fácilmente desde el sistema Guardium (servidor GIM).

Consulte el tema sobre instalación de GIM en el servidor de base de datos (Unix) y sobre Guardium Installation Manager (GIM) - GUI para obtener más información sobre cómo instalar y utilizar GIM para instalar los componentes de Guardium en un entorno Windows.
Nota: Si se utiliza A-Tap, este se debe inhabilitar en el servidor de base de datos antes de realizar una actualización o desinstalación de S-TAP mediante GIM.
Nota: En un entorno IBM DB2 pureScale, se debe poder acceder a perl durante un rearranque para garantizar que se inicia S-TAP.

Mantenimiento de S-TAP de UNIX sin GIM

Mantenimiento de S-TAP de Unix sin GIM

Aunque se ha proporcionado GIM para facilitar la instalación y la gestión de componentes de Guardium, todavía hay entornos que pueden beneficiarse de un enfoque más manual o de un ajuste de la instalación a un nivel más granular. La sección siguiente se proporciona para esos entornos.

- Instalación de S-TAP de Unix
- Instalación de S-TAP desde la línea de mandatos
- Instalación de CAS desde la línea de mandatos
- Actualización del programa de utilidad del procedimiento
- Eliminación del S-TAP de Unix anterior (manual)
- Actualización de línea de mandatos para K-Tap (manual)
- Detención de S-TAP de Unix
- Reinicio de S-TAP de Unix
- Determinación del número de versión de S-TAP de Unix
- Utilización de los instaladores nativos de S-TAP de Unix

Detención de S-TAP de Unix

En función del método de instalación de S-TAP, puede detener S-TAP de una de estas formas:

Instalación de GIM

Puede utilizar GIM para detener S-TAP sin tener que iniciar la sesión en el servidor de base de datos. Siga los pasos siguientes para cambiar el parámetro STAP_ENABLED y planificar el cambio en el servidor de base de datos.

1. Pulse Gestionar > Gestión de instalación > Configurado por cliente (Antiguo) para abrir los Criterios de búsqueda de cliente.
2. Realice una búsqueda filtrada de clientes registrados o pulse Buscar para ver todos los clientes registrados.
3. Seleccione los clientes que serán el destino de la acción (al detener S-TAP).
   - Si hay más de 20 clientes, la lista de clientes se divide en páginas adicionales.
     Nota: Si se pulsa el botón Seleccionar todo, solo se seleccionarán los clientes de la página actual que se está visualizando.
4. Pulse Siguiente para abrir el panel Módulos comunes.
5. Seleccione el módulo para S-TAP.
6. Pulse el botón Siguiente para abrir el panel Parámetros de módulo.
7. Seleccione el cliente que será el destino de la acción (al detener S-TAP).
8. Cambie el parámetro STAP_ENABLED por 0 (cero).
9. Pulse Aplicar a clientes para que se aplique a los clientes de destino.
10. Pulse el botón Instalar/Actualizar para planificar la actualización de los clientes de destino. Esta actualización se puede planificar para ahora o para un momento futuro.

En el propio host de la base de datos, puede detener S-TAP (y todos los módulos GIM excepto el propio GIM) deteniendo el servicio supervisor de GIM con el mandato: stop gsvr_<release number>. Utilice initctl list para obtener la lista de los estados de los servicios.

Instalación no GIM

1. Inicie la sesión en el sistema del servidor de base de datos utilizando la cuenta root.
2. Para todos los sistemas que no sean Hat Enterprise Linux 6
   a. Abra el archivo /etc/inittab para editarlo.
   b. Localice y comente las dos sentencias siguientes en el archivo /etc/inittab, mediante la inserción de un carácter de comentario (*:* para AIX, # para todos los demás) al principio de cada sentencia:

      ```
      utap:2345:respawn:/usr/local/guardium/guard_stap/guard_stap /usr/local/guardium/guard_stap/guard_tap.ini
      ```

   c. Opcional. Si está utilizando el mecanismo de supervisión TEE, comente las dos sentencias siguientes insertando un carácter de comentario (dos puntos *:* para AIX, signo de almohadilla # para todos los demás) al principio de cada sentencia.
      Nota: Estos procesos no se utilizan en la configuración predeterminada, de modo que es posible que las sentencias ya estén comentadas.

      ```
      #utee:2345:respawn:/usr/local/guardium/guard_stap/guard_tee /usr/local/guardium/guard_stap/guard_tap.ini
      #hsof:2345:respawn:/usr/local/guardium/guard_stap/guard_hnt
      ```

   d. Ejecute el mandato init q para reiniciar los procesos de S-TAP.
3. Para Red Hat Enterprise Linux 6.
   a. Obtenga una lista de los agentes que se están ejecutando actualmente con el mandato initctl list del sistema operativo. La salida muestra los agentes que se listan como en el ejemplo siguiente:

      ```
      gim_33264 start/running, process 910
      gsvr_33264 start/running, process 2552
      ```

   b. Detenga cada uno de los agentes que pueda estar en ejecución con el mandato stop <agent>, donde agent sería la primera entrada de la lista del paso 3a.

      ```
      stop gim_33264
      stop gsvr_33264
      stop guard_utap
      ```

      Utilice stop guard_utap para detener el S-TAP o stop guard_tee para detener el mecanismo TEE del agente S-TAP.

4. Ejecute ps -ef | grep stap para comprobar que los procesos de S-TAP se han detenido.
5. En el portal del administrador del sistema Guardium al que notificaba este S-TAP, verifique que la luz de estado del panel de control de S-TAP es ahora de color rojo.

Reinicio de S-TAP de Unix

En función del método de instalación de S-TAP, puede reiniciar S-TAP de una de estas formas:

Instalación de GIM

Utilice GIM para iniciar S-TAP sin tener que iniciar la sesión en el servidor de base de datos. Siga los pasos siguientes para cambiar el parámetro STAP_ENABLED y planificar el cambio en el servidor de base de datos.

1. Pulse Gestionar > Gestión de instalación > Configurado por cliente (Antiguo) para abrir los Criterios de búsqueda de cliente.
2. Realice una búsqueda filtrada de clientes registrados o pulse Buscar para realizar una búsqueda no filtrada de todos los clientes registrados.
3. Seleccione los clientes que serán el destino de la acción (al iniciar S-TAP).
   - Si hay más de 20 clientes, la lista de clientes se divide en páginas adicionales.
     Nota: Si se pulsa Seleccionar todo, solo se seleccionarán los clientes de la página actual que se está visualizando.
4. Pulse Siguiente para abrir el panel Módulos comunes.
5. Seleccione el módulo para S-TAP.
6. Pulse Siguiente para abrir el panel Parámetros de módulo.
7. Seleccione el cliente que será el destino de la acción (al iniciar S-TAP).
8. Cambie el parámetro STAP_ENABLED por 1 (uno).
9. Pulse Aplicar a clientes para que se aplique a los clientes de destino.
10. Pulse Instalar/Actualizar para planificar la actualización de los clientes de destino. Esta actualización se puede planificar para ahora o para un momento futuro.

Instalación no GIM

1. Inicie la sesión en el sistema del servidor de base de datos utilizando la cuenta root.
2. Para todos los sistemas que no sean Hat Enterprise Linux 6

a. Abra el archivo /etc/inittab para editarlo.
b. Suprima el comentario de las dos sentencias siguientes suprimiendo el carácter de comentario (*:* para AIX, # para todos los demás) al principio de cada línea:

```
#utap:2345:respawn:/usr/local/guardium/guard_stap/guard_stap /usr/local/guardium/guard_stap/guard_tap.ini
```

c. Opcional. Si está utilizando el mecanismo de supervisión TEE, suprima el comentario de las dos sentencias siguientes suprimiendo el carácter de comentario (*:* para AIX, # para todos los demás) al principio de cada sentencia.
Nota: Estos procesos no se utilizan en la configuración predeterminada y no se deben iniciar si utiliza el mecanismo de supervisión K-Tap.

```
#utee:2345:respawn:/usr/local/guardium/guard_stap/guard_tee /usr/local/guardium/guard_stap/guard_tap.ini
#hsof:2345:respawn:/usr/local/guardium/guard_stap/guard_hnt
```

d. Ejecute el mandato init q para reiniciar los procesos de S-TAP.

3. Para Red Hat Enterprise Linux 6.
a. Obtenga una lista de los agentes que se están ejecutando actualmente con el mandato initctl list del sistema operativo. La salida muestra los agentes que se listan como en el ejemplo siguiente:

```
gim_33264 start/running, process 910
gsvr_33264 start/running, process 2552
```

b. Inicie cada uno de los agentes con el mandato start <agent>, donde agent sería la primera entrada de la lista del paso a. Consulte el siguiente ejemplo.

```
start gim_33264
start gsvr_33264
start guard_utap
```

4. Ejecute ps -ef | grep stap para comprobar que S-TAP se está ejecutando.
5. En el portal del administrador del sistema Guardium al que notifica este S-TAP, verifique que la luz de estado del panel de control de S-TAP es de color verde.

Detenga y reinicie S-TAP mediante los servicios de Solaris en Solaris 10 y 11

Solaris 10 y 11 ya no utilizan inittab. En su lugar, se utilizan los servicios de Solaris para detener e iniciar el S-TAP. Utilice el programa de utilidad svcadm.

Detener

```
-bash-3.00# svcadm -v disable guard_utap
svc:/site/guard_utap:default disabled.
-bash-3.00# ps -eaf | grep stap
    root  2375  1930   0 14:25:36 pts/2       0:00 grep stap
```

Reiniciar

```
-bash-3.00# svcadm -v enable guard_utap
svc:/site/guard_utap:default enabled.
-bash-3.00# ps -eaf | grep stap
 root  2379     1   0 14:25:57 ?           0:00
/usr/local/guardium/guard_stap/guard_stap /usr/local/guardium/guard_stap/guard_
    root  2396  1930   0 14:26:00 pts/2       0:00 grep stap
-bash-3.00# svcs guard_utap
STATE          STIME    FMRI
online         14:25:56 svc:/site/guard_utap:default
-bash-3.00#
```

Plugin de Kerberos para S-TAP de UNIX

Kerberos es un protocolo de autenticación de red. Está diseñado para proporcionar una autenticación sólida para las aplicaciones cliente/servidor utilizando criptografía de clave secreta.

Presenta las características siguientes:

- Es seguro: nunca envía una contraseña a menos que esté cifrada.
- Sólo se necesita un inicio de sesión por sesión. Las credenciales definidas durante el inicio de sesión se pasan entre los recursos sin necesidad de inicios de sesión adicionales.
- El concepto depende de un tercero de confianza, un centro de distribución de claves (KDC). El KDC reconoce todos los sistemas de la red y es de confianza para todos ellos.
- Realiza la autenticación mutua, donde un cliente demuestra su identidad ante un servidor y un servidor demuestra su identidad ante el cliente.

Para poder capturar un usuario autenticado de Kerberos, se necesita un-S-TAP. Ahora Guardium incluye un plugin de Kerberos que forma parte del S-TAP. Este plugin requiere una configuración adicional.

El usuario debe localizar las bibliotecas de Kerberos del sistema. Las bibliotecas necesarias suelen ser:

libgssapi_krb5.so

libkrb5.so

libk5crypto.so

libkrbsupport.so

Todas estas bibliotecas deben estar en las vías de acceso de biblioteca estándar. Si, por cualquier motivo, no lo están, el método recomendado es crear enlaces simbólicos. Si esto no es posible, existe una solución temporal que se describirá más adelante.

1. El plugin de Kerberos de STAP no está habilitado de forma predeterminada y lo debe habilitar el usuario especificando el valor correspondiente a "kerberos_plugin_dir" en el archivo de configuración "guard_tap.ini" de STAP.

   Para la instalación de shell de S-TAP, kerberos_plugin_dir=<guardium_base>/guard_stap, y para la instalación de GIM, kerberos_plugin_dir=<guardium_base>/modules/STAP/current

2. El paso siguiente consiste en configurar los parámetros en el archivo "guardkerbplugin.conf" que también se encuentra en el directorio de instalación de S-TAP.

   KRB5_KTNAME=<vía acceso al archivo krb5.keytab de kerberos>

   KRB5_CONFIG=<vía acceso al archivo krb5.conf de kerberos>

   KRB5_PLUGIN_CCACHE=<vía acceso al archivo krb5cc_* de kerberos> parámetro opcional para el método alternativo si el plugin de Kerberos no ha reconocido al usuario por alguna razón

   Para Oracle Kerberos, estos valores se encuentran en el archivo “sqlnet.ora”

   Ejemplo:

   ~]$ grep -i KERBEROS $ORACLE_HOME/network/admin/sqlnet.ora

   SQLNET.AUTHENTICATION_KERBEROS5_SERVICE = oracle

   SQLNET.KERBEROS5_CONF = /home/oracle11/krb5/krb5.conf

   SQLNET.KERBEROS5_REALMS = /home/oracle11/krb5/krb.realms

   SQLNET.AUTHENTICATION_SERVICES= (BEQ,KERBEROS5)

   SQLNET.KERBEROS5_CLOCKSKEW = 600

   SQLNET.KERBEROS5_KEYTAB = /home/oracle11/krb5/keytab

   SQLNET.KERBEROS5_CONF_MIT = TRUE

   Tenga en cuenta que en este caso no se ha especificado este parámetro de memoria caché, pero se puede encontrar con el mandato siguiente:

   ~]$ oklist|grep -i cache

   Ticket cache: /tmp/krb5cc_500

   Para Sybase Kerberos, de las variables de entorno de Sybase o “klist -k”, “klist -c”

   Ejemplo:

   env|grep -i KRB

   KRB5_KTNAME=/home/sybase15/kerberos/keytab

   KRB5_CONFIG=/home/sybase15/kerberos/krb5.conf

   klist -c

   Ticket cache: FILE:/tmp/krb5cc_533

   Default principal: sybuser1@GUARD.SWG.USMA.IBM.COM

   Valid starting Expires Service principal

   05/17/16 15:04:29 05/17/16 21:44:29 krbtgt/GUARD.SWG.USMA.IBM.COM@GUARD.SWG.USMA.IBM.COM

   klist -k

   Keytab name: FILE:/home/sybase15/kerberos/keytab

Si las bibliotecas de Kerberos NO están en las vías de acceso de biblioteca estándar.

Se han implementado nuevos parámetros para el plugin de Kerberos y se tienen que establecer en "guardkerbplugin.conf"

KRB5_PLUGIN_GSSAPI_LIBRARY=<vía acceso completa a libgssapi_krb5.so>

La vía de acceso a las bibliotecas de Kerberos se puede encontrar buscando en el sistema de archivos

Ejemplo:

bash-4.2# find / -name libgssapi_krb5.so

/opt/freeware/lib/libgssapi_krb5.so

/opt/freeware/lib64/libgssapi_krb5.so

En este caso se han encontrado dos bibliotecas, “/opt/freeware/lib/libgssapi_krb5.so” es la biblioteca de 32 bits y solo se puede utilizar en sistemas de 32 bits y “/opt/freeware/lib64/libgssapi_krb5.so” es la biblioteca de 64 bits y se debe utilizar en bibliotecas de 64 bits

Suponiendo que el sistema es de 64 bits, la configuración de Kerberos se establecerá de la siguiente manera:

Kerberos values

KRB5RCACHETYPE=none

KRB5_KTNAME=/home/sybase16/kerberos/keytab

KRB5_CONFIG=/home/sybase16/kerberos/krb5.conf

Plugin values

KRB5_PLUGIN_CCACHE=/home/sybase16/krb5cc_sybase16

KRB5_PLUGIN_GSSAPI_LIBRARY=/opt/freeware/lib64/libgssapi_krb5.so

#KRB5_PLUGIN_DEBUG=0

Temas "Cómo..." de S-TAP de UNIX

Cómo determinar el número de versión de S-TAP de UNIX

Cómo determinar los parámetros de DB2

Cómo encontrar el tamaño de segmento de la memoria compartida de DB2

Cómo acceder a las estadísticas de S-TAP

Cómo determinar el número de versión de S-TAP de UNIX

En el portal de administrador de un servidor de Guardium para un S-TAP, el número de versión de S-TAP se muestra en el informe Supervisor de estado de S-TAP en el separador Vista del sistema.

Si el portal de administrador no está disponible, puede visualizar el número de versión de S-TAP desde la línea de mandatos del servidor de base de datos, ejecutando el binario guard_stap con el argumento -version o --version.

Para comprobar la versión de S-TAP de UNIX, suponiendo que S-TAP se ha instalado en el directorio de instalación predeterminado, especifique el mandato siguiente:

```
-bash-3.2#  <guardium_base>/modules/STAP/current/guard_stap --version
o
-bash-3.2#  <guardium_base>/guard_stap/guard_stap --version
STAP-doberman_r20511_1-20100728_0514
```

Cómo determinar los parámetros de DB2

La interceptación de DB2 en S-TAP se basa en los parámetros siguientes:

Tabla 2. Parámetros de DB2

Parámetro	Nombre de STAP	Nombre ATAP	Valor predeterminado	Comentario
Tamaño de cabecera de paquete	db2_fixed_pack_adjustment	db2_header_offset	20	El valor predeterminado se ha probado para DB2 8.2 y posteriores en diversas plataformas de 64 bits. Es posible que otras versiones de DB2 y plataformas de 32 bits necesiten un desplazamiento distinto. Los sospechosos habituales son 16 y 12.
Desplazamiento del área de E/S de cliente	db2_shmem_client_position	db2_c2soffset	61440	Este parámetro se deriva del parámetro DB2 ASLHEAPSZ.
Tamaño de segmento de memoria compartida de DB2	db2_shmem_size	db2_shmsize	131072	Este parámetro se determina empíricamente. Consulte una secuencia de mandatos que se puede utilizar para obtenerlo.

Nota: Si hay varias instancias de DB2 configuradas para una sola WPAR en el archivo guard_tap.ini y tienen el mismo db2_shmem_size, entonces se devolverán los valores de db2_fix_pack_adjustment y db2_shmem_client_position configurados en la primera sección de DB2 para esa WPAR. Por lo tanto, si hay varias instancias de DB2 en ejecución en la WPAR:

1. Si todas las instancias de DB2 tienen los mismos valores de db2_shmem_size, db2_fix_pack_adjustment y db2_shmem_client_position, se recopilarán los paquetes de todas las instancias aunque sólo se haya configurado una instancia.
2. Si todas las instancias de DB2 tienen el mismo db2_shmem_size, pero diferentes db2_fix_pack_adjustment o db2_shmem_client_position, sólo se recopilarán los paquetes de la primera instancia de DB2 configurada.

Desplazamiento del área de E/S del cliente de cálculo (db2_shmem_client_position)

1. Abra un nuevo shell bash como usuario de la instancia de db2.
2. Ejecute el mandato ps -x para verificar que el procesador de mandatos de db2bp no se está ejecutando actualmente para este shell. No debería ver el mandato denominado db2bp en ejecución. Si lo ve, puede interrumpirlo o ejecutar un nuevo shell.
3. Ejecute los dos mandatos siguientes:

```
db2 get database manager configuration | awk '/ASLHEAPSZ/{print $9 * 4096}'
```

La salida es el valor necesario para db2_shmem_client_position.

El parámetro ASLHEAPSZ se especifica en páginas de memoria de 4K en DB2. Determina el tamaño del almacenamiento dinámico de la capa de soporte de la aplicación. Tal como se muestra en el diagrama anterior, el área de E/S del cliente se inicia después del almacenamiento dinámico de la aplicación en el segmento de memoria compartida del agente/aplicación.

Nota: La teoría detrás de este cálculo se basa en el manual IBM DB2 Universal Database Administration Guide: Performance. En el diagrama siguiente se muestra el diseño de la memoria compartida de DB2.

Cómo encontrar el tamaño de segmento de la memoria compartida de DB2

ATAP y KTAP se basan en el tamaño para la identificación de los segmentos de memoria compartida de la aplicación/agente. Luego se interviene en estos segmentos mediante paquetes C2S y S2C.

Siga estos pasos para encontrar el tamaño del segmento:

1. Inicie una conexión de memoria compartida de DB2 y manténgala abierta.
2. Ejecute este mandato para obtener el ID de proceso para db2sysc: ps -eaf | grep db2sysc. La salida se parece a la siguiente:

   ```
   db2inst1  5309370  5505772   0   Nov 11      - 1232:12 db2sysc 0
   ```

   En este ejemplo, el ID de proceso es 5309370.
3. Ejecute este mandato para recuperar información sobre los procesos de memoria compartida: ipcs -ma La salida se parece a la siguiente:

   ```
   IPC status from /dev/mem as of Wed Nov 20 13:21:45 CST 2013
   T         ID     KEY        MODE       OWNER    GROUP  CREATOR   CGROUP NATTCH     SEGSZ  CPID
   m    2097152 0xffffffff D-rw------- pconsole   system pconsole   system      1 536870912 4522088
   m          1 0x78000015 --rw-rw-rw-     root   system     root   system      3  16777216 3605314
   m          2 0x78000016 --rw-rw-rw-     root   system     root   system      3 268435456 3605314
   m  219152387 0xffffffff D-rw-------     root   system     root   system      1 536870912 5243842
   m    1048580 0x61013002 --rw------- pconsole   system pconsole   system      1  10485760 4522088
   m   10485765 0xd9fd8a61 --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      5  47644672 5571082
   m    9437190 0xd9fd8a74 --rw-rw-rw- db2inst1 db2iadm1 db2inst1 db2iadm1      9 140852104 5571082
   m    9437191 0xe1bd8858 --rw-rw----   oracle      dba   oracle      dba     40 53687107584 3801352
   m    3145736 0x52594801 --rw-rw----     root informix     root informix     13 223019008 5702650
   m    3145737 0xd9fd8b68 --rw-rw---- db2inst1 db2iadm1 db2inst1 db2iadm1      1  58720256 6619354
   m    3145738 0xffffffff --rw------- db2fenc1 db2fadm1 db2inst1 db2iadm1      7 268435456 5505772
   m         11 0x52594802 --rw-rw----     root informix     root informix     13  33439744 5702650
   m         12 0x52594803 --rw-rw-rw-     root informix     root informix     13    573440 5702650
   m         13 0xf2033f7e --rw------- sybase15   sybase sybase15   sybase      1 115564544 5178168
   m  409993231 0x52594804 --rw-rw---- informix informix informix informix     13   8388608 5702650
   m  763363344 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 268435456 5309370
   m  125829140 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      2    131072 5309370
   m  201326613 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 163905536 5309370
   m  103750230 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 134217280 5309370
   ```

   La salida contiene varias columnas más de las que se muestran aquí, pero no afectan a este procedimiento. Busque la línea que contiene el ID de proceso que se ha identificado en el paso 2 y que también tiene el valor 2 bajo NATTCH. El tamaño de segmento de memoria compartida de DB2 es el valor de la columna SEGSZ. En este ejemplo, es 131072.
4. Sugerencia: si la lista devuelta en el paso 3 es demasiado larga, puede filtrarla utilizando el ID de proceso. En este caso, debería especificar ipcs -ma | grep 5309370. Los resultados no contienen las cabeceras de columna, pero puede mirar los resultados anteriores para ver las cabeceras de columna e identificar la línea y columna correctas. En este ejemplo, es la última línea.

   ```
   m 131072014 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 1342177280 5309370
   m 763363344 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 268435456 5309370
   m 227541013 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      1 163905536 5309370
   m 106353238 0xffffffff --rw------- db2inst1 db2iadm1 db2inst1 db2iadm1      2    131072 5309370
   ```

Utilice el siguiente procedimiento alternativo para un método más fácil, pero menos preciso, para encontrar el tamaño de segmento de memoria compartida de DB2 (db2_shmem_size):

Los segmentos equivalen a la suma de los parámetros ASLHEAPSZ y RQRIOBLK. DB2 asigna segmentos mucho mayores. En la mayoría de los casos, el tamaño es igual a (ASLHEAPSZ + 1) * 2 páginas, o (ASLHEAPSZ + 1) * 8192 bytes. El tamaño exacto se puede determinar observando los segmentos de memoria compartidos en el sistema antes y después de que se cree una nueva conexión local de DB2.

Utilice esta secuencia de mandatos para determinar el tamaño del segmento de memoria compartida.

Los parámetros del mandato ipcs y el formato de salida difieren de plataforma a plataforma. El script siguiente se basa en la versión de AIX.

```
ipcs -ma | sort -n -2 +3 > /tmp/before.txt
db2 connect to <some_existing_database>ipcs -ma | sort -n -2 +3 > /tmp/after.txt
db2 terminate
diff /tmp/before.txt /tmp/after.txt | awk '{if ($10 == 2) print $11}'
```

Siempre es aconsejable verificar el resultado. Es igual o al menos parecido al de la salida del mandato siguiente:

```
db2 get database manager configuration | awk '/ASLHEAPSZ/{print ($9 + 1) * 8192}'
```

Cómo acceder a las estadísticas de S-TAP

Acceda a la tabla STAP_Statistic para que el usuario pueda crear alertas basadas en resultados.

Esta tabla se utiliza para almacenar las estadísticas que S-TAP envía al sniffer.

No hay ningún informe predefinido para esta tabla.

Intervalo de tiempo en horas (ejemplo, 5 es cada 5 horas)

Utilice - (menos) para un intervalo de tiempo de menos de 1 hora.

Campos de la tabla

TIMESTAMP

SOFTWARE_TAP_HOST

TOTAL_BYTES_SO_FAR

TOTAL_BYTES_DROPPED_SO_FAR

TOTAL_BYTES_IGNORED

TOTAL_BUFFER_INIT

IOCTL_REQUESTS

TOTAL_RESPONSE_BYTES_IGNORED

System CPU%

System Idle%

STAP CPU%

Buffer recycled

Tema principal: S-TAPs y otros agentes

S-TAP de Windows

Utilice esta sección para ver información de configuración de S-TAP de Windows.

Novedades de V10

Imágenes nativas (de 32 / 64 bits)

Nuevos controladores TCP y NP (WFP, NmpMonitor)

Windows Filtering Platform (WFP) sustituye a los controladores TCP basados en TDI (interfaz de controlador de transporte).

Wfpmonitor es el nuevo controlador TCP de S-TAP, que sustituye a lhmonproxy y lhmon.

WFP ofrece las siguientes ventajas:

- Se puede actualizar sin necesidad de rearrancar
- No es necesario reiniciar las instancias de base de datos para recoger el tráfico TCP después de una instalación
- Ahora todos los controladores proporcionan un recurso de registro (cíclico). Los archivos de registro se encuentran en /logs. Esto mejora la capacidad de soporte, ya que los errores/avisos del controlador no estaban visibles.

El controlador de conductos con nombre se ha rediseñado. Ahora se divide en proxy y supervisor: NmpProxy y NmpMonitor, en sustitución de Nptrc. De esta forma se divide la funcionalidad en basic-OS (NmpProxy) y Guardium-logic (NmpMonitor).

Inicio de S-TAP de Windows

En función del método de instalación de S-TAP, puede iniciar S-TAP haciendo lo siguiente:

Instalación de GIM

GIM le permite iniciar S-TAP sin tener que iniciar una sesión en el servidor de base de datos. Siga los pasos siguientes para cambiar el parámetro WINSTAP_ENABLED y planificar el cambio en el servidor de base de datos.

1. Pulse Gestión de instalación > Configurado por cliente (Antiguo) para abrir los Criterios de búsqueda de cliente.
2. Pulse Buscar para realizar una búsqueda filtrada.
3. Seleccione los clientes que serán el destino de la acción (al iniciar S-TAP)
4. Pulse Siguiente para abrir el panel Módulos comunes.
5. Seleccione el módulo para WINSTAP.
6. Pulse Siguiente para abrir el panel Parámetros de módulo.
7. Seleccione el cliente que será el destino de la acción (al iniciar S-TAP).
8. Cambie el parámetro WINSTAP_ENABLED por 1 (uno).
9. Pulse Aplicar a clientes para que se aplique a los clientes de destino.
10. Pulse Instalar/Actualizar para planificar la actualización de los clientes de destino. Esta actualización se puede planificar para ahora o para un momento futuro. Cuando se ejecute la planificación para esta actualización, se iniciará el servicio S-TAP en los clientes de destino.

Instalación no GIM

1. Inicie una sesión en el sistema servidor de base de datos mediante una cuenta de administrador del sistema.
2. En el panel de control Servicios, inicie el servicio GUARDIUM_STAP.
3. Inicie una sesión en el sistema Guardium al que notifica este S-TAP. Verifique que la luz de estado del panel de control de S-TAP es de color verde.

Nota: Cuando el S-TAP de Windows encuentra un error muy grave durante el inicio que se debe a problemas de configuración (dirección IP local desconocida, más de 1 SQL-Guards primario definido, etc.) registrará la razón en el registro de sucesos de Windows. En algunos casos, una salida después de una anomalía puede provocar un bloqueo y otro suceso registrado. Este bloqueo no debería causar ningún problema si está precedido por el suceso que explica la razón de la anomalía.

Detención de S-TAP de Windows

En función del método de instalación de S-TAP, puede detener S-TAP haciendo lo siguiente:

Instalación de GIM

GIM le permite detener S-TAP sin tener que iniciar una sesión en el servidor de base de datos. Siga los pasos siguientes para cambiar el parámetro WINSTAP_ENABLED y planificar el cambio en el servidor de base de datos.

1. Pulse Gestión de instalación > Configurado por cliente (Antiguo) para abrir los Criterios de búsqueda de cliente.
2. Especifique los criterios de búsqueda de cliente si desea realizar un búsqueda filtrada de clientes registrados.
3. Pulse Buscar para realizar una búsqueda filtrada y visualizar el panel Clientes.
4. Seleccione los clientes que serán el destino de la acción (al detener S-TAP).
5. Pulse Siguiente para abrir el panel Módulos comunes.
6. Seleccione el módulo para WINSTAP.

7. Pulse Siguiente para abrir el panel Parámetros de módulo.
8. Seleccione el cliente que serán el destino de la acción (al detener S-TAP)
9. Cambie el parámetro WINSTAP_ENABLED por 0.
10. Pulse Aplicar a clientes para que se aplique a los clientes de destino
11. Pulse Instalar/Actualizar para planificar la actualización de los clientes de destino. Esta actualización se puede planificar para ahora o para un momento futuro. Cuando se ejecute la planificación para esta actualización, se detendrá el servicio S-TAP en los clientes de destino.

Instalación no GIM

1. Inicie una sesión en el sistema servidor de base de datos mediante una cuenta de administrador del sistema.
2. En el panel de control Servicios:
   - Detenga el servicio GUARDIUM_STAP.
3. Inicie una sesión en la interfaz de usuario del sistema Guardium al que notifica este S-TAP y verifique que la luz de estado del panel de con trol de S-TAP es ahora roja.

Reconfiguración de CAS de la ubicación de JAVA_HOME

En muchos casos, el programa de instalación se encarga de buscar el valor de JAVA_HOME. Este valor se coloca en el archivo de configuración de CAS.

Si, por algún motivo (por ejemplo, si instala una nueva versión de Java™ después de instalar el producto Guardium CAS), debe cambiar la ubicación de JAVA_HOME, siga el procedimiento siguiente.

1. Localice y abra el archivo de configuración de CAS para editarlo. Su nombre de vía de acceso completo es: <installation directory>/case/conf/wrapper.conf
2. Localice la siguiente entrada: `wrapper.java.command=<value>`
3. Sustituya value por el directorio JAVA_HOME
4. Guarde el archivo.

CAS y el registro de Windows de 64 bits

En Windows, los parámetros de configuración de software se almacenan en el árbol de registro en la clave HKEY_LOCAL_MACHINE\SOFTWARE. Puesto que una máquina de 64 bits puede ejecutar versiones de 64 bits y de 32 bits de la misma aplicación, es necesario distinguir los parámetros de configuración de las aplicaciones de 64 bits y de 32 bits.

La solución de Microsoft al problema consiste en particionar el registro. Se ha añadido una clave especial, denominada WOW6432Node, al árbol de registro en la clave HKEY_LOCAL_MACHINE\SOFTWARE. Cuando una aplicación de 32 bits intenta acceder al registro a través de una vía de acceso dentro de la clave HKEY_LOCAL_MACHINE\SOFTWARE, Windows inserta la clave especial WOW6432Node en la vía de acceso. De este modo, la aplicación de 32 bits se ocupa del registro de Windows igual que lo haría en una máquina de 32 bits, y Windows se encarga de redirigirlo a la partición correcta.

CAS es una aplicación Java de 32 bits, por lo que normalmente no tendrá acceso a los parámetros de configuración de software de 64 bits. CAS se ha mejorado para detectar un entorno de 64 bits y manejar el registro particionado. El interés de CAS en el registro es recuperar valores de las claves de registro para detectar cambios o para compararlos con los valores recomendados.

Como ejemplo, supongamos que CAS debe recuperar el valor de HKEY_LOCAL_MACHINE\SOFTWARE\MyApp\Parameter1. Ese valor podría corresponder a cualquier partición, a ambas o a ninguna. Si corresponde a ninguna partición, CAS recuperará un valor nulo. De lo contrario, devuelve una serie que es la concatenación de los dos valores separados por la serie WOW6432Node. Si el valor está en la partición de 64 bits pero no en la de 32 bits, la serie recuperada se parecería a Value64WOW6432Nodenull. Por el contrario, si el valor está en la partición de 32 pero no en la de 64 bits, la serie de caracteres sería nullWOW6432NodeValue32. Por último, si el valor se encuentra en ambas particiones, la serie devuelta sería Value64WOW6432NodeValue32. Esta nueva búsqueda de patrón de valor de registro buscará ambas particiones del registro cuando corresponda.

Recopilación de SID del recopilador del dominio

GuardiumDC es un servicio que recopila actualizaciones de las cuentas de usuario (SID y nombres de usuario) del controlador de dominio primario y marca los cambios en Guardium_S-TAP para actualizar la correlación entre SID interno y nombre de usuario de S-TAP. Si S-TAP no encuentra un SID resuelto en la correlación, intenta obtenerlo del controlador de dominio primario, en cuyo caso el S-TAP registra un mensaje en el registro de depuración (nivel 7): `El nombre de cuenta *** se ha recuperado para SID ***`.

DC_COLLECT_FREQ en la sección TAP especifica la frecuencia de la recopilación en horas, con un mínimo de 1 y un máximo de 24 (valor predeterminado).

DC_COLLECT_MAXUSERS en la sección TAP especifica el número máximo de usuarios que se deben recopilar, el valor predeterminado es 200.000, el mínimo es 10.000.

Ejemplo de DOMAIN_CONTROLLER: DOMAIN_CONTROLLER=\\atari.

Implementación de la modalidad de usuario de memoria compartida de DB2

Hay dos formas de capturar el tráfico de la memoria compartida de DB2 mediante el S-TAP de Windows.

En el sistema Guardum, elimine la marca de DB2 en el menú S-TAPCONTROL > Supervisor de memoria compartida > DB2.

Utilice el TAP: (márquelo).

En los detalles (CONTROL de Guardium S-TAP) > Supervisor de memoria compartida > TAP debe estar marcado.

(Si ambos métodos están marcados, se utilizará el método DB2 TAP).

En el motor de inspección de S-TAP, se necesita el nombre de instancia de DB2 (encontrará el nombre de instancia en el Panel de control-> Servicios->nombre, la instancia es la última parte del nombre de servicio de DB2. Por ejemplo, si el nombre de servicio para DB2 es DB2-DB2COPY1-DB2-0, el nombre de la instancia será DB2-0. Hay un programa de utilidad db2TAP.exe en el directorio Guardium. Ejecute db2tap.exe list en una ventana de mandatos para ver el nombre de la instancia.

Ejemplo de motor de inspección:

```
[DB_DB21]
PORT_RANGE_START=50001
PORT_RANGE_END=50001
DB2_FIX_PACK_ADJUSTMENT=80
```

```
INSTANCE_NAME=DB2_01-0
DB_TYPE=DB2
NETWORKS=1.1.1.1/0.0.0.0
```

Parámetros de memoria compartida de DB2

Ajuste de memoria compartida de DB2 / Posición de cliente de memoria compartida de DB2

Valores de los parámetros de memoria compartida de DB2 en Windows:

DB2_FIX_PACK_ADJUSTMENT
: El valor predeterminado de este parámetro es 80 decimal. Debería ser correcto para DB2 versiones 8.2 y posteriores. Para versiones anteriores, pruebe 20 decimal.

DB2_CLIENT_OFFSET
: El valor predeterminado para este parámetro es 61440 decimal. Este parámetro se calcula tomando el valor de configuración de base de datos DB2 de ASLHEAPSZ y multiplicándolo por 4096.

  Para obtener el valor de ASLHEAPSZ, ejecute el siguiente mandato de DB2: db2 get dbm cfg y busque el valor de ASLHEAPSZ. Este valor suele ser 15, que da como resultado el valor predeterminado 61440. Si no es 15, multiplique el valor por 4096 para obtener el desplazamiento de cliente adecuado.

Integración de DB2 Exit con S-TAP de Windows

Cuando se utilizan los releases de DB2 10.1 y posteriores, el S-TAP captura todo el tráfico de DB2 directamente desde el motor de DB2. Cuando se utiliza este método, no se da soporte a la funcionalidad de limpieza/redacción (scrub/redact). Además, los procedimientos almacenados no se capturan. Todo el tráfico de DB2 se captura, independientemente del protocolo de cifrado/red. Esta solución simplifica la configuración de S-TAP para los clientes que despliegan esta versión de DB2 y les proporciona soporte de DB2 nativo. Siga estos pasos para configurar el S-TAP para este tipo de base de datos:

1. 1. Cree una nueva carpeta en la carpeta DB2 SQLLIB para cada instancia $DB2PATH\security\plugin\commexit\instance_name Por ejemplo: C:\Program Files\IBM\SQLLIB\security\plugin\commexit\DB2_01
2. Copie las DLL correspondientes del directorio de instalación de S-TAP en los directorios creados:
   Para DB2 de 32 bits:
   - db2fexitx86.dll
   - db2exitx86.dll

   Para DB2 de 64 bits:
   - db2exitx64.dll
   - db2fexitx64.dll
3. Detenga la instancia o instancias de DB2 y emita el mandato siguiente:

   UPDATE DBM CFG USING COMM_EXIT_LIST db2fexitx86 (para 32 bits)

   UPDATE DBM CFG USING COMM_EXIT_LIST db2fexitx (para 64 bits)

4. Inicie las instancias de DB2.
5. Añada un motor de inspección para la DB2 Exit

   En la sección TAP:

   DB2_EXIT_DRIVER_INSTALLED=1

   La sección DB refleja el nuevo tipo de motor de inspección:

   [DB_DB2_EXIT1]

   DB_TYPE=DB2_EXIT

   INSTANCE_NAME=Service_name

   El nombre de servicio no es el nombre de la instancia. Puede determinar el nombre de servicio mediante el programa de utilidad db2tap en la carpeta de instalación de S-TAP o desde el panel de control. Establezca el nombre de instancia en la parte del nombre de servicio que hay detrás del segundo delimitador de guión (-). Por ejemplo, si el nombre de servicio en el panel de control es `DB2-DB2COPY1-DB2-01-0`, establezca INSTANCE_NAME en `DB2-01-0`.

6. Para dejar de utilizar la característica y detener DB2, emita el mandato siguiente y vuelva a iniciar DB2: db2 UPDATE DBM CFG USING COMM_EXIT_LIST NULL

Estadísticas de S-TAP

Acceda a la tabla STAP_Statistic para que el usuario pueda crear alertas basadas en resultados.

Esta tabla se utiliza para almacenar las estadísticas que S-TAP envía al sniffer.

No hay ningún informe predefinido para esta tabla.

Intervalo de tiempo en horas (ejemplo, 5 es cada 5 horas)

Utilice - (menos) para un intervalo de tiempo de menos de 1 hora.

Campos de la tabla

TIMESTAMP

SOFTWARE_TAP_HOST

TOTAL_BYTES_SO_FAR

TOTAL_BYTES_DROPPED_SO_FAR

TOTAL_BYTES_IGNORED

TOTAL_BUFFER_INIT

IOCTL_REQUESTS

TOTAL_RESPONSE_BYTES_IGNORED

System CPU%

System Idle%

STAP CPU%

Buffer recycled

Tema principal: S-TAPs y otros agentes

S-TAP Discovery

Habilite S-TAP para descubrir de forma periódica instancias de bases de datos y enviar los resultados al sistema S-TAP activo actual.

Visión general

Utilice la aplicación Guardium S-TAP Discovery para descubrir instancias de bases de datos de forma periódica y enviar las instancias al sistema S-TAP activo actual. Si el S-TAP se está ejecutando como usuario, la funcionalidad de descubrimiento será limitada. Aparece el siguiente mensaje:

```
AVISO: El descubrimiento está habilitado y STAP se está ejecutando como usuario guardium. La función de descubrimiento está
limitada cuando STAP se ejecuta como usuario guardium. El descubrimiento es más efectivo cuando 'tap_run_as_root=1'
```

Nota: S-TAP Discovery no recibe soporte en AIX 5.3 porque se necesitan bibliotecas estáticas en esa plataforma.
Nota: Para evitar una instancia en la que el descubrimiento de S-TAP no abre la base de datos Informix, se recomienda iniciar las bases de datos utilizando la vía de acceso completa al ejecutable.

Bases de datos soportadas con S-TAP Discovery

Oracle, DB2, Informix, MySQL, PostgreSGL, Sybase. Hadoop, Teradata, Netezza, MemSQL

Los parámetros de la aplicación de descubrimiento S-TAP se describen en Parámetros de descubrimiento.

El descubrimiento también utiliza estos parámetros:

- tap_ip: S-TAP al que se asocia la instancia de la base de datos.
- sqlguard_ip: Los resultados del descubrimiento de S-TAP se envían a esta dirección IP. (El sistema de Guardium con primary=1 en los parámetros de SQLguard.)

Si se está ejecutando un descubrimiento planificado, y llega una nueva solicitud procedente de la interfaz de usuario para ejecutar el descubrimiento, la nueva solicitud se pasa por alto.

Configuración

La aplicación S-TAP Discovery utiliza el archivo de configuración de UNIX, guard_tap.ini, para su configuración. El archivo tiene varios de sus propios parámetros de configuración en el archivo y se basa en los parámetros para funcionar.

S-TAP Discovery se puede ejecutar manualmente, pero esta acción no se recomienda. La razón principal de ejecutarla manualmente es para fines de depuración.

Para enviar los resultados al sistema Guardium, utilice la vía de acceso de archivo <vía acceso absoluta al binario de guard_discovery>/guard_discovery<vía acceso a guard_tap.ini>/guard_tap.ini o <vía acceso absoluta al binario de guard_discovery>/guard_discovery <vía acceso a guard_tap.ini>/guard_tap.ini --send-to-sqlguard

Para imprimir los resultados en stdout, utilice el mandato <vía acceso absoluta al binario de guard_discovery>/guard_discovery <vía acceso a guard_tap.ini>/guard_tap.ini --print-output.

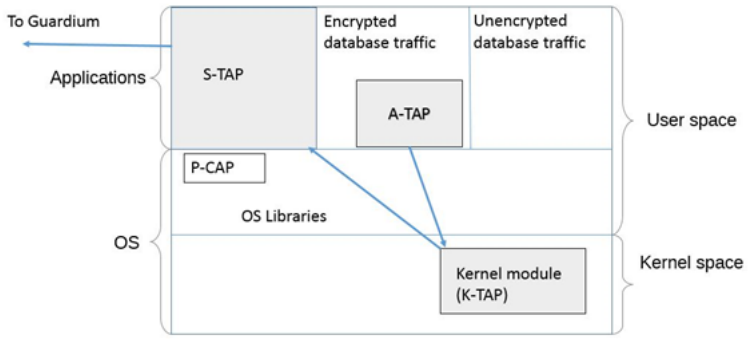
Tema principal: S-TAPs y otros agentes

Gestión de A-TAP

A-TAP es una abreviación de TAP a nivel de aplicación (Application-level TAP). Un A-TAP se ubica en la capa de la aplicación para dar soporte a la supervisión del tráfico de base de datos cifrado, lo que no es posible realizar en el kernel mediante un K-TAP.

Un mecanismo de A-TAP (TAP a nivel de aplicación) supervisa la comunicación entre los componentes internos del servidor de base de datos. Los datos no están cifrados en la capa de la aplicación, donde el A-TAP los recoge y los envía a un K-TAP. Un K-TAP es un proxy que pasa datos al S-TAP, y desde allí se envía entonces al recopilador de Guardium.

Esta imagen muestra la ubicación de los A-TAP dentro de la arquitectura general en el servidor de base de datos.



Un A-TAP se incluye en cada S-TAP, sin embargo, debe ser configurado específicamente para cada base de datos que lo precise.

Cuándo utilizar un ATAP

Se necesita un A-TAP cuando se utiliza cifrado DBMS (no Windows). Pueden haber otros detalles de implementación de base de datos internos como, por ejemplo, memoria compartida que lo precise.

Informix y DB2 en Linux se integran en mayor con medida con Guardium utilizando salidas y, por lo tanto, son el método recomendado para el soporte a la memoria compartida cuando así corresponda.

Restricciones: No se da soporte a los A-TAP en un entorno donde una base de datos de 32 bits se encuentra ubicada en un servidor de 64 bits.

Restricciones de supervisión: Los A-TAP no dan soporte a la redacción. Se da soporte a los bloqueos para kernels de Linux versión 2.6.36 o posteriores.

- Preparación para la configuración y el mantenimiento de A-TAP
  Para configurar y realizar el mantenimiento de A-TAP se requiere una coordinación tanto con la base de datos como con los administradores del sistema.
- Configuración y activación de A-TAP
  Configure y active cada A-TAP.
- Directrices para la activación y desactivación de A-TAP y para la detención y reinicio de la BD
  Comprenda cuándo se debe activar y desactivar A-TAP, y detener o reiniciar la base de datos.
- Mandatos del programa de utilidad guardctl para A-TAP
  El programa de utilidad guardctl es una herramienta de gestión de A-TAP. Examine estos mandatos antes de empezar a trabajar con los A-TAP.
- Códigos de retorno de guardctl
  Los códigos de error de guardctl clarifican las condiciones de error que se producen, en concreto cuando se llama al script guardctl para gestionar instancias de ATAP a través de otro script.
- Parámetros de guardctl específicos de la base de datos
  Cada tipo de base de datos tiene requisitos específicos de guardctl.
- Desactivación de A-TAP
  Debe desactivar A-TAP antes de actualizar el sistema operativo de la base de datos
- Configuración y activación de A-TAP en entornos especiales
  Las zonas, WPAR, Teradata y Oracle requieren una configuración adicional.
- Resolución de problemas de configuración de A-TAP
  Esta sección contiene un resumen de los errores comunes que se realizan durante las configuraciones de A-TAP, sus síntomas y cómo evitarlos.

Tema principal: S-TAPs y otros agentes

Preparación para la configuración y el mantenimiento de A-TAP

Para configurar y realizar el mantenimiento de A-TAP se requiere una coordinación tanto con la base de datos como con los administradores del sistema.

Para configurar y activar A-TAP, se necesitan las autoridades siguientes:

- Acceso root sobre el servidor de base de datos
- Autoridad para detener y reiniciar la base de datos

Además, debe trabajar con el administrador de la base de datos para obtener los parámetros necesarios que deberá especificar en el programa de utilidad. Encontrará los detalles de los parámetros necesarios en Parámetros de guardctl específicos de la base de datos. Para el mantenimiento continuado, la organización debe tener procedimientos documentados para manejar la activación y desactivación de A-TAP durante las actualizaciones del sistema operativo y base de datos. Consulte Directrices para la activación y desactivación de A-TAP y para la detención y reinicio de la BD. Para entornos en clúster, es necesario configurar y activar A-TAP en todos los nodos.

En la mayoría de los casos, utilice el programa de utilidad de Guardium guardctl para activar, actualizar o desactivar A-TAP. También puede implementar un script de derivador (wrapper) para utilizar guardctl como interfaz de programa de utilidad para ATAP, que proporciona su propia experiencia de usuario. Consulte Mandatos del programa de utilidad guardctl para A-TAP para ver detalles sobre la sintaxis y las opciones del programa de utilidad guardctl.

Antes de empezar:

- Asegúrese de que el S-TAP esté instalado y de que K-TAP esté habilitado.
- Asegúrese de que tiene privilegios de root sobre el servidor de bases de datos.
- Consulte Parámetros de guardctl específicos de la base de datos para su base de datos para asegurarse de que tiene los parámetros que necesita para ejecutar el programa de utilidad.

Tema principal: Gestión de A-TAP

Configuración y activación de A-TAP

Configure y active cada A-TAP.

Acerca de esta tarea

Requisito previo: S-TAP debe estar instalado.

Procedimiento

1. Compruebe que aparece ktap_installed=1 en el archivo guard_tap.ini.
2. Finalice la sesión de todas las sesiones de base de datos activas y detenga la base de datos. Es muy importante que todos los procesos con el usuario administrador de la base de datos se detengan. Por ejemplo, en oracle, emita ps -ef | grep oracle
3. Como usuario root, autorice al usuario administrativo de la base de datos a registrar el tráfico utilizando el programa de utilidad guardctl con el mandato autor-user del siguiente modo:
   `<guardium_base>/xxx/guardctl authorize-user <user-name>`

   Ejemplo de instalador de shell

   ```
   /usr/local/guardium/guard_stap/guardctl authorize-user postgres
   Autorizando al usuario 'postgres' a registrar el tráfico
   ```

   Ejemplo de verificación de autorización

   ```
   /usr/local/guardium/guard_stap/guardctl is_user_authorized postgres
   El usuario 'postgres' está autorizado.
   ```

   Ejemplo de instalación de GIM

   ```
   /usr/local/guardium/modules/ATAP/current/files/bin/guardctl authorize_user postgres
   Autorizando al usuario 'postgres' a registrar el tráfico
   ```

4. Almacene los parámetros de configuración:
   a. Consulte Parámetros de guardctl específicos de la base de datos para determinar los parámetros necesarios para el tipo y plataforma de la base de datos.
   b. Como usuario root, almacene la configuración para la instancia de base de datos con el mandato store-conf del programa de utilidad guardctl de la siguiente manera:
   `<guardium_base>/xxx/guardctl db_instance=<instance> [<name>=<value> ...] store-conf`

   Ejemplo de instalador de shell de Oracle en Linux: /usr/local/guardium/guard_stap/guardctl --db-user=oracle11 --db-type=oracle --db-instance=on12rh60 --db-home=/home/oracle11/product/11.1.0/db_1 --db-version=11.2 store-conf
   Ejemplo de instalación de Oracle en GIM de Linux: /usr/local/guardium/modules/ATAP/current/files/bin/guardctl db_instance=$ORACLE_SID db_home=$ORACLE_HOME db_type=oracle db_user=oracle12 db_version=12 store-conf

   Nota: En Guardium V10.1 y posteriores, la instrumentación se realiza automáticamente durante la activación; no hay ninguna instrumentación explícita.
5. Active A-TAP.
   a. Como usuario root, especifique `<guardium_base>/xxx/guardctl db_instance=<instance> activate`

      Ejemplo de instalador de shell

      ```
      /usr/local/guardium/guard_stap/guardctl --db-instance=onrh60x activate
      ```

      Ejemplo de instalación de GIM

      ```
      /usr/local/guardium/modules/ATAP/current/files/bin/guardctl --db-instance=onrh60x activate
      ```

      Nota: Si lo desea, puede activar A-TAP utilizando el recuadro de selección Cifrado de la configuración del motor de inspección de la GUI de Guardium, aunque no ofrece ninguna ventaja sobre activarlo en la GUI. Esta opción no está disponible para plataformas Linux.
   b. Confirme que las instancias se activan mediante el mandato list-active del programa de utilidad guardctl: <guardium_base> /xxx/guardctl list-active

      Ejemplo: <guardium_base>/xxx/guardctl list-active oracle

6. Reinicie el servidor de base de datos.

Tema principal: Gestión de A-TAP

Directrices para la activación y desactivación de A-TAP y para la detención y reinicio de la BD

Comprenda cuándo se debe activar y desactivar A-TAP, y detener o reiniciar la base de datos.

Requisitos para el reinicio, carga, instrumentación y activación para A-TAP

Escenario	Instrucciones
Después de la instalación de A-TAP de UNIX en un entorno de clúster de Oracle	todas las instancias de base de datos, así como todos los procesos entre clústeres, se deben reiniciar
Antes de activar A-TAP	Detener la base de datos
Después de activar A-TAP	Reiniciar la base de datos
Antes de desactivar A-TAP	Detener la base de datos
Antes de actualizar la base de datos (por ejemplo, aplicar un fixpack)	Desactivar A-TAP
Antes de actualizar S-TAP	Desactivar A-TAP

Tema principal: Gestión de A-TAP

Mandatos del programa de utilidad guardctl para A-TAP

El programa de utilidad guardctl es una herramienta de gestión de A-TAP. Examine estos mandatos antes de empezar a trabajar con los A-TAP.

Programa de utilidad guardctl

Para utilizar el programa de utilidad guardctl, debe iniciar la sesión como **root**, ya que requiere privilegios de superusuario. El programa de utilidad guardctl se instala en el directorio <guardium_base>/guard_stap, donde <guardium_base> es el directorio en el que está instalado el software de Guardium. En el caso de un mandato guardctl de instalación de GIM, se instala bajo <guardium_base>/modules/ATAP/current/files/bin.

Sintaxis

<guardium_base>/xxx/guardctl [<parameter>=value>] [<parameter>=<value> ...] <command> [-q | -v | -qv]

Consulte los parámetros en Parámetros de guardctl específicos de la base de datos.

-q, -v, -qv flags

En Guardium V10.1.3, utilice estos distintivos para gestionar la salida:

- -q (quiet): suprimir toda la salida excepto los pares de nombre/valor
- -v (pares de valores): añadir pares de nombre/valor relacionados con cada mandato
- -qv: sólo genera pares de nombre/valor

La salida depende del tipo de mandato.

- Mandatos que emprenden acciones en todas las instancias configuradas
  - Imprimir todos los pares de nombre/valor para cada instancia, excepto overall_rv y overall_msg
  - Imprima el par nombre/valor overall_rv en el extremo en el que se encuentra el valor
    - 0 (correcto) si y solo si todo el informe ha sido satisfactorio
    - 1 (error) si hay algún error en algún informe
  - Imprimir el par nombre/valor de overall_msg al final
  - Devuelve el valor notificado en el par de nombre/valor "overall_rv"
- Mandatos que emprenden acciones en una sola instancia
  - Imprimir todos los pares de nombre/valor, excepto overall_rv y overall_msg
  - Devuelve el valor notificado en el par de nombre/valor "rv"
- Mandatos que almacenan parámetros, imprimen parámetros o comprueban el estado
  - No imprime pares de nombre/valor

La salida de los pares de nombre/valor tiene el siguiente aspecto:

```
db_instance: ${db_instance}
db_user: ${db_user}
db_base: ${db_base}
db_home: ${db_base}
db_version: ${db_version}
db_type: ${db_type}
is_active: ${is_active} (“yes” or “no”)
is_instrumented: ${is_db_instrumented} (“yes” or “no”)
msg: some string
rv: ${retval}
overall_rv: ${retval}
overall_msg: (string)
```

Mandatos

Mandato	Descripción
activate	Activa el A-TAP correspondiente a la instancia de base de datos especificada utilizando los parámetros almacenados. La salida son los pares de nombre/valor si se especifica -v o -qv. A partir de Guardium V10.1.3, la activación de una instancia que ya está activa (tanto si la base de datos se está ejecutando como si no) no genera un error.
authorize-user	Añade el usuario al grupo de autorización 'guardium'.
deactivate	Desactiva el A-TAP para la instancia de base de datos única especificada. La salida son los pares de nombre/valor si se especifica -v o -qv. A partir de Guardium V10.1.3, la desactivación de una instancia que ya está inactiva (tanto si la base de datos se está ejecutando como si no) no genera un error.
deactivate-all	Desactiva el A-TAP correspondiente a una lista especificada de instancias de base de datos. Si no se especifica ninguna instancia de base de datos, se desactivan todos los TAP activos. La salida son los pares de nombre/valor para cada instancia si se especifica -v o -qv. Opcionalmente, puede especificar db-type para desactivar un grupo (por ejemplo, todo Oracle). Para un par de nombre/valor adicional, especifique "overall_rv ={0,1}" al final. Devuelve Correcto (0) si rv=0 para cada instancia. Devuelve Error (1) si al menos una instancia devuelve rv!=0.
deinstrument	Elimina la instrumentación para la base de datos Oracle especificada. No es necesario para V10.1 y posteriores. Si es necesaria la desinstrumentación, se realiza automáticamente durante la desactivación. La salida son los pares de nombre/valor si se especifica -v o -qv. A partir de Guardium V10.1.3, la desinstrumentación de una instancia que no está instrumentada no genera un error, aunque la base de datos se esté ejecutando, independientemente del estado de activación.
dump-params	Realiza un volcado de los valores actuales de los parámetros
get-statistics	Obtener estadísticas de A-TAP.
help	Mandato predeterminad, muestra la lista de mandatos y parámetros admitidos y de sus valores predeterminados
instrument	Crea de forma explícita la información de Oracle instrumentada. Si es necesaria la instrumentación, normalmente se realiza automáticamente durante la activación. La instrumentación manual sólo es necesaria para las versiones de Oracle <=10 en AIX. La instrumentación de una instancia ya instrumentada devuelve un error. La salida son los pares de nombre/valor si se especifica -v o -qv.
is-active	Devuelve 1 si hay al menos una instancia de A-TAP activada. De lo contrario, devuelve 0.

Mandato	Descripción
is-user-authorized	Comprueba si db-user (que ejecuta A-TAP) está autorizado para registrar el tráfico de la base de datos en K-TAP/S-TAP.
list-active	Muestra una lista de los nombres de usuario de la instancia de base de datos de todas las instancias de base de datos de A-TAP activas. La salida son los pares de nombre/valor si se ha especificado -v o -qv.
list-configured	Muestra una lista de las instancias de base de datos con A-TAP configurados pero inactivos. La salida son los pares de nombre/valor si se especifica -v o -qv.
oracle-relink	db-exec vuelve a enlazar Oracle
prepare-libs	Prepara bibliotecas para utilizas en la instalación de zona/WPAR
repair	Ejecute este mandato si la base de datos se actualiza (accidentalmente) mientras el ATAP está activo. Separa los archivos -guard-original y -guard-instrumented. Devuelve Correcto si la reparación se ha realizado correctamente o si no es necesaria ninguna reparación. No afecta al ejecutable de la base de datos actual. Devuelve los pares de nombre/valor si se especifica -v o -qv.
restore-active-ataps	Restaura el estado activo de los ATAP previamente guardados mediante save-active-ataps. Si una instancia no se puede activar (debido a que se está ejecutando la base de datos o a algún otro error), se sigue intentando activar las instancias restantes. Este mandato se puede ejecutar varias veces sin problema, ya que la activación de una instancia que ya está activa no es un error. Se ha introducido en Guardium V10.1.4.
save-active-ataps	Guarda las configuraciones de los ATAP activos actualmente en un único archivo de forma que se puedan restaurar más tarde a un estado activo. Resulta de utilidad antes de ejecutar deactivate-all al preparar la actualización de las BD. Se ha introducido en Guardium V10.1.4.
store-conf	Almacena la configuración correspondiente a una instancia de base de datos determinada
store-system-conf	Almacena los parámetros de configuración del sistema

Tema principal: Gestión de A-TAP

Códigos de retorno de guardctl

Los códigos de error de guardctl clarifican las condiciones de error que se producen, en concreto cuando se llama al script guardctl para gestionar instancias de ATAP a través de otro script.

Código	Descripción	Uso
0	correcto	Lo devuelve cada mandato. Cuando se devuelve en respuesta a una desactivación, se desactivan todas las instancias Cuando se devuelve en respuesta a is-active, no hay instancias activas
1	parámetro erróneo	Lo devuelve cada mandato cuando falta un parámetro o no es válido
2	Se ha llamado a is-active en una instancia no reconocida	Lo devuelve is-active cuando guardctl no conoce una db-instance especificada y por tanto no puede determinar si está activa o no
20	se ha intentado activar una instancia mientras se estaba ejecutando la base de datos, pero todavía no está activa	Lo devuelve el mandato activate para indicar que la instancia de base de datos se está ejecutando, por lo que no se ha podido llevar a cabo la activación
21	se ha intentado desactivar una instancia mientras se estaba ejecutando la base de datos, pero todavía no está inactiva	Lo devuelve el mandato deactivate para indicar que la instancia de base de datos se está ejecutando, por lo que no se ha podido llevar a cabo la desactivación
22	el usuario no está autorizado	Lo devuelven los mandatos instrument y activate para indicar que el db-user especificado no tiene autorización como miembro del grupo 'guardium'. Ejecute authorize-user para corregirlo.
23	El parámetro db-home no coincide con el parámetro db_install_dir en guard_tap.ini	Lo devuelven los mandatos store-conf y activate para indicar que el archivo guard_tap.ini actual no tiene configurado un IE con un db_home que coincida con el parámetro de ATAP db_install_dir. Se tiene que ajustar uno de estos para corregir el valor o STAP no se podrá ejecutar.
24	se ha intentado desactivar una instancia en la que el ejecutable no es un ejecutor de ATAP ni el binario instrumentado	Lo devuelve el mandato deactivate. Parece que esta instancia debería activarse, pero el binario no es el que debería ser si lo estuviera. Es posible que se haya actualizado el ejecutable de la BD mientras ATAP estaba activo. Ejecute el mandato repair para solucionar el problema y activar de nuevo.
25	se ha intentado activar atap cuando encryption= 1 estaba establecido en guard_tap.ini	Lo devuelve el mandato activate cuando el parámetro encryption está establecido en 1 en el IE. No lo active con guardctl y utilice el parámetro encryption en el archivo ini.
26	no se ha encontrado el archivo ejecutable de la bd	Lo devuelven los mandatos activate, deactivate, instrument, deinstrument, store-conf, prepare-libs y repair. Falta el ejecutable de la base de datos (es decir, el propio binario oracle no está en la vía de acceso especificada). Compruebe los parámetros de vía de acceso utilizados al configurar la instancia.
27	instrumentación necesaria pero no realizada	Lo devuelven los mandatos activate y store-conf cuando se necesita una instrumentación pero aún no se ha llevado a cabo. Ahora la instrumentación de Oracle se realiza automáticamente en la mayoría de los casos, pero se debe especificar manualmente para las versiones de AIX y Oracle <= 10.
28	el mandato is-active muestra que la instancia no está activa	Lo devuelve el mandato is-active. Solo informativo. La instancia de base de datos especificada no está activa o, si no se ha especificado ninguna instancia, no hay ninguna instancia activa.
29	deactivate-all no ha sido del todo correcto	Lo devuelve el mandato deactivate-all cuando al menos una instancia activa no se ha podido desactivar.
30	is-instrumented muestra que la instancia no está instrumentada	No se ha exportado mediante el mandato.

Código	Descripción	Uso
40	error interno de instrumentación	Lo devuelve el mandato instrument cuando no se ha podido completar la instrumentación.
41	error interno de instrumentación	Lo devuelve el mandato instrument cuando no se ha podido completar la instrumentación.
42	error interno de instrumentación	Lo devuelve el mandato instrument cuando no se ha podido completar la instrumentación.
43	error de instrumentación, no se ha podido guardar el binario original	Lo devuelve el mandato instrument cuando el archivo -guard-original ya existe. A-TAP está actualmente activo con instrumentación o bien A-TAP está inactivo pero la instrumentación sigue activa. Desactive y desinstrumente antes de la siguiente instrumentación y activación.
44	se ha intentado instrumentar mientras se estaba ejecutando la instancia y aún no estaba instrumentada	Lo devuelve el mandato instrument cuando la instancia de base de datos se está ejecutando actualmente. Detenga la instancia de base de datos antes de intentar instrumentarla de nuevo.
45	se ha intentado instrumentar mientras A-TAP estaba activo y aún no estaba instrumentado	Lo devuelve el mandato instrument cuando A-TAP ya está activo, pero la instrumentación no está activa. Esto puede suceder cuando se pasa de una configuración de Oracle que no requiere instrumentación a una que sí la requiere. Desactive el A-TAP antes de intentar instrumentarlo de nuevo.
46	se ha intentado instrumentar una instancia que ya estaba instrumentada	Lo devuelve el mandato instrument cuando la instancia ya está instrumentada. Si es necesario volver a realizar la instrumentación, primero debe desinstrumentar.
94	no hay ninguna biblioteca atap que dé soporte esta base de datos	Lo devuelven los mandatos instrument, deinstrument, prepare-libs, activate, deactivate, repair, list-active y list-configured. Normalmente indica que se ha producido un error desconocido.
93	error no especificado porque base de datos se está ejecutando cuando no se está activando, desactivando o instrumentando (por ejemplo, cuando se ejecuta el mandato de reparación)	
95	error del sistema, no se puede encontrar el grupo	Lo devuelve el mandato activate. Parece que el sistema no reconoce el grupo de guardium.
96	error del sistema, no se puede crear el grupo	Lo devuelve el mandato authorize-user. El grupo de guardium no existía y ha fallado un intento de crear el grupo.
97	error del sistema de archivos, no se puede crear el archivo o el archivo o se ha detectado que no hay suficiente espacio	
98	plataforma no soportada	Lo devuelven los mandatos instrument, deinstrument, prepare-libs, activate, deactivate, repair, list-active, list-configured, store-conf. La base de datos que está intentando utilizar con ATAP no recibe soporte en esta plataforma (por ejemplo, DB2, Informix, teradata o mongo en cualquier plataforma que no sea Linux, etc).
99	otro error no especificado	

Tema principal: Gestión de A-TAP

Parámetros de guardctl específicos de la base de datos

Cada tipo de base de datos tiene requisitos específicos de guardctl.

- Parámetros de guardctl específicos de Oracle
  Utilice estos parámetros de guardctl cuando configure A-TAP para una base de datos Oracle.
- Parámetros de guardctl específicos de Sybase
  Utilice estos parámetros de guardctl cuando configure A-TAP para una base de datos Sybase.
- Parámetros de guardctl específicos de DB2 (solo Linux)
  Utilice estos parámetros de guardctl cuando configure A-TAP para una base de datos DB2 (solo Linux).
- Parámetros de guardctl específicos de Informix
  Utilice estos parámetros de guardctl cuando configure A-TAP para una base de datos Informix.
- Parámetros de guardctl específicos de Postgres
  Utilice estos parámetros de guardctl cuando configure A-TAP para una base de datos Postgres.

Tema principal: Gestión de A-TAP

Parámetros de guardctl específicos de Oracle

Utilice estos parámetros de guardctl cuando configure A-TAP para una base de datos Oracle.

Ejemplo:

/usr/local/guardium/guard_stap/guardctl --db-user=oracle11 --db-type=oracle --db-instance=on12rh60 --db-home=/home/oracle11/product/11.1.0/db_1 --db-version=11.2 store-conf

Parámetros obligatorios de Oracle

Parámetro obligatorio	Valor	Cómo se determina
db-user	Nombre del usuario de Oracle	Utilice el nombre de usuario de la instancia de base de datos.
db_instance	Nombre de la instancia de Oracle	Utilice el valor de $ORACLE_SID
db_type	Oracle	
db_home	Donde está instalado el ejecutable de la base de datos.	

Parámetro obligatorio	Valor	Cómo se determina
db_base	Directorio de inicio del usuario de la instancia de la base de datos	El valor de db_base debe coincidir con la vía de acceso correcta para $ORACLE_BASE o con el directorio de inicio del usuario de la instancia de la base de datos. No puede ser ~DB_USER.
db_version	La versión de la base de datos	Ejecute SQL > SELECT * FROM V$VERSION

Parámetros opcionales de Oracle

Parámetro opcional	Valor	Cómo se determina	Cuándo se necesita
db_relink	No/yes	Método de activación de A-TAP	
db_use_instrumented	No/yes	La activación de A-TAP utiliza la versión vuelva a vincular de Oracle creada anteriormente con el mandato de instrumentación de guardctl.	Se necesita instrumentación para: • Oracle 12 SSL en todas las plataformas que no sean Windows • Oracle 11.2 SSL en AIX • Oracle ASO y SSL en AIX anterior a 11.2 **Importante:** con un S-TAP al nivel 10.1, la instrumentación se realiza automáticamente con el mandato “activate” o mediante la interfaz de usuario de Guardium.
db_bits	32 o 64	Arquitectura de la instancia de la BD (32 para 32 bits, 64 para 64 bits)	Sólo es necesario si A-TAP no puede reconocer la arquitectura.

Tema principal: Parámetros de guardctl específicos de la base de datos

Parámetros de guardctl específicos de Sybase

Utilice estos parámetros de guardctl cuando configure A-TAP para una base de datos Sybase.

Parámetros obligatorios de Sybase

Ejemplo:

/usr/local/guardium/guard_stap/guardctl --db-user=sybase15 --db-type=sybase --db-instance=sn57rh7x --db-version=15 store-conf

Parámetro obligatorio	Valor	Cómo se determina
db_user	Nombre del usuario de Sybase	Utilice el nombre de usuario de la instancia de base de datos.
db_instance	Nombre de la instancia de Sybase	Nombre de la instancia del servidor Sybase
db_type	sybase	
db_version	La versión de la base de datos	Como usuario de Sybase: > select @@version > go

Parámetros opcionales de Sybase

Parámetro opcional	Valor	Cómo se determina	Cuándo se necesita
db_home	Apunta a donde está instalada la base de datos	Igual que db_base	
db_base	Directorio de inicio del usuario de la instancia de la base de datos	Directorio de inicio del usuario de la instancia de BD. El valor de db_base debe coincidir con el directorio de inicio del usuario de la instancia de BD de la vía de acceso correcta. No puede ser ~DB_USER.	Donde db_base no es igual que db_home.
db_bits	32 o 64	Arquitectura de la instancia de la BD (32 para 32 bits, 64 para 64 bits)	Sólo es necesario si A-TAP no puede reconocer la arquitectura.
db-tcp-min-port	Entre 0 y cualquier entero	Límite inferior del rango de puertos TCP a interceptar	Se utilizan IP reales
db-tcp-max-port	Entre 0 y cualquier entero	Límite superior del rango de puertos TCP a interceptar	Se utilizan IP reales

Tema principal: Parámetros de guardctl específicos de la base de datos

Parámetros de guardctl específicos de DB2 (solo Linux)

Utilice estos parámetros de guardctl cuando configure A-TAP para una base de datos DB2 (solo Linux).

Parámetros obligatorios de DB2 (solo Linux)

Ejemplo:

/usr/local/guardium/guard_stap/guardctl --db-user=db2inst1 --db-type=db2 --db-instance=dn0rh7x6 --db-version=10.5 store-conf

Parámetro obligatorio	Valor	Cómo se determina
db_user	Nombre de usuario de DB2	Apunta al nombre de usuario de la instancia de la BD
db_instance	Nombre de la instancia de DB2	$ db2 LIST DATABASE DIRECTORY
db_type	db2	
db_version	La versión de la base de datos	Como usuario de DB2: $ db2level

Parámetros opcionales de DB2 (solo Linux)

Parámetro opcional	Valor	Cómo se determina	Cuándo se necesita
db_home	Vía de acceso en la que está instalada la versión de la BD	Igual que db_base	
db_base	Directorio de inicio del usuario de la instancia de la base de datos	El valor de db_base debe coincidir con el directorio de inicio del usuario de la instancia de BD de la vía de acceso correcta. No puede ser ~DB_USER.	Donde db_base no es igual que db_home
db_bits	32 o 64	Arquitectura de la instancia de la BD (32 para 32 bits, 64 para 64 bits)	Sólo es necesario si A-TAP no puede reconocer la arquitectura.
db2-shmsize	131072	Tamaño de la memoria compartida de DB2	Cuando el valor es distinto del valor predeterminado
db2-c2soffset	61440	Desplazamiento del área de cliente de la memoria compartida de DB2	Cuando el valor es distinto del valor predeterminado
db2-header-offset	20	Desplazamiento de cabecera de memoria compartida de DB2	Cuando el valor es distinto del valor predeterminado

Tema principal: Parámetros de guardctl específicos de la base de datos

Parámetros de guardctl específicos de Informix

Utilice estos parámetros de guardctl cuando configure A-TAP para una base de datos Informix.

Parámetros obligatorios de Informix

Ejemplo:

/usr/local/guardium/guard_stap/guardctl --db-user=informix --db-type=informix --db-instance=in17rh7x --db-version=11.70 store-conf

Parámetro obligatorio	Valor	Cómo se determina
db_user	Nombre de usuario de Informix	Apunta al nombre de usuario de la instancia de la BD
db_instance	Nombre de la instancia de Informix	Nombre de instancia del servidor de Informix
db_type	informix	
db_version	La versión de la base de datos	Como usuario de Informix: dbaccess -V

Parámetros opcionales de Informix

Parámetro opcional	Valor	Cómo se determina	Cuándo se necesita
db_home	Vía de acceso en la que está instalada la versión de la BD	Igual que db_base	
db_base	Directorio inicial de db_user	Directorio de inicio del usuario de la instancia de BD. El valor de db_base debe coincidir con el directorio de inicio del usuario de la instancia de BD de la vía de acceso correcta. No puede ser ~DB_USER.	Donde db_base no es igual que db_home
db_bits	32 o 64	Arquitectura de la instancia de la BD (32 para 32 bits, 64 para 64 bits)	

Tema principal: Parámetros de guardctl específicos de la base de datos

Parámetros de guardctl específicos de Postgres

Utilice estos parámetros de guardctl cuando configure A-TAP para una base de datos Postgres.

Parámetros obligatorios de Postgres

Ejemplo:

/usr/local/guardium/guard_stap/guardctl --db-user=postgres --db-type=postgres --db-instance=guardium_qa --db-version=9.4 --db-base=/home/postgres94 store-conf

Parámetro obligatorio	Valor	Cómo se determina
db-user	Nombre de usuario de Postgres	Apunta al nombre de usuario de la instancia de la BD
db_instance	Nombre de instancia de Postgres	Nombre de la instancia del servidor Postgres
db_type	postgres	
db_version	La versión de la base de datos	Como usuario de Postgres: pg_ctl --version

Parámetros opcionales de Postgres

Parámetro opcional	Valor	Cómo se determina	Cuándo se necesita
db_home	Apunta a donde está instalada la versión de la BD	Igual que db_base	
db_base	Directorio inicial de db_user	Directorio de inicio del usuario de la instancia de BD. El valor de db_base debe coincidir con el directorio de inicio del usuario de la instancia de BD de la vía de acceso correcta. No puede ser ~DB_USER.	Donde db-base no es igual que db-home
db_bits	32 o 64	Arquitectura de la instancia de la BD (32 para 32 bits, 64 para 64 bits)	
db-tcp-min-port	Entre 0 y cualquier entero	Límite inferior del rango de puertos TCP a interceptar	Se utilizan IP reales
db-tcp-max-port	Entre 0 y cualquier entero	Límite superior del rango de puertos TCP a interceptar	Se utilizan IP reales

Tema principal: Parámetros de guardctl específicos de la base de datos

Desactivación de A-TAP

Debe desactivar A-TAP antes de actualizar el sistema operativo de la base de datos

Acerca de esta tarea

Procedimiento

1. Asegúrese de que la base de datos se haya detenido. Finalice la sesión de todas las sesiones de base de datos activas.
2. Desactive A-TAP para la base de datos:
   `<guardium_base>/xxx/guardctl –db-instance=<instance-name> deactivate`
3. Como alternativa, puede desactivar todas las instancias activas ejecutando este mandato:
   `<guardium_base>/xxx/guardctl deactivate-all`

Tema principal: Gestión de A-TAP

Configuración y activación de A-TAP en entornos especiales

Las zonas, WPAR, Teradata y Oracle requieren una configuración adicional.

- Instalación y activación de A-TAP en entornos de zonas y WPAR
- Desactivación y desinstalación de A-TAP en entornos de zonas y de WPAR
- Actualización de ATAP en entornos de zonas y WPAR
- Pasos para configurar y activar A-TAP para una base de datos Teradata
- Configuración de Oracle para A-TAP

Tema principal: Gestión de A-TAP

Instalación y activación de A-TAP en entornos de zonas y WPAR

Acerca de esta tarea

Procedimiento

1. Instale STAP/KTAP en la zone/WPAR maestro/global con el método normal.
2. Para las zonas de Solaris, para cada subzona donde esté instalado Oracle asegúrese de que el dispositivo Guardium® esté correlacionado:
   - zoneadm -z <zonename> halt
   - zonecfg -z <zonename>
   - <zonename>> add device
   - <zonename>device> set match=/dev/ktap_xxx (for Solaris 10)
   - <zonename>device> set match=/dev/guard_ktap (for Solaris 11)
   - <zonename>device> end
   - <zonename>> verify

- <zonename>> exit
- zoneadm -z <zonename> boot

3. Si hay varios dispositivos KTAP, repita los pasos para cada dispositivo KTAP utilizando el nombre ktap_xxxx (Solaris 10) o guard_ktap_x (Solaris 11).
4. Copie todo el directorio de instalación de A-TAP en una subzona/subWPAR. Suponiendo que el software Guardium esté instalado en la zona/WPAR maestra bajo /usr/local/guardium y que existe un directorio /usr/local en el que se puede escribir con suficiente espacio libre en la subzona/WPAR, en la zona/WPAR maestra/global: `cd /usr/local; tar -cvf - guardium | ssh root@subzonehost 'cd /usr/local && tar -xvf -'`
5. Copie las bibliotecas de A-TAP en cada subzona/subWPAR y actívelas.
   - Si se tiene que activar un A-TAP en la zona/WPAR maestra, actívelo como lo haría normalmente mediante guardctl.
     Nota: La activación debe realizarse mediante guardctl; no se puede hacer mediante la habilitación del recuadro de cifrado en la sección del motor de inspección en la interfaz de la GUI ni estableciendo encryption= 1 en el archivo guard_tap.ini.
   - Si no se va a utilizar un A-TAP en la zona/WPAR maestra, utilice guardctl para preparar las bibliotecas para su uso. En la zona/WPAR maestra:
     `/usr/local/guardium/bin/guardctl --db_instance=<instance-name> --db_type=<database-type> --db_version=<database-version> prepare-libs`
     Nota: Después de la activación de A-TAP, si la base de datos indica que no se ha encontrado libguard-xxx.so, vuelva a comprobar este paso.
6. Instale y active A-TAP para las instancias de la base de datos mediante 1 a 5 en cada subzona/subWPAR.
   Nota: Es posible que una activación de A-TAP (guardctl) se queje y emita avisos sobre lo siguiente:
   - errores al instalar bibliotecas bajo /usr/lib (puesto que este directorio pertenece a la zona global/maestra)
   - no puede cambiar guard_tap.ini para supervisar oracle-guard en lugar de oracle
   - no puede reiniciar stap (ya que sólo se está ejecutando en la zona maestra)
7. Ajuste el archivo guard_tap.ini en la zona/WPAR maestra/global de forma manual editando el archivo guard_tap.ini.
   - Cambie la línea db_exec_path adecuada:
     - Para Oracle en Solaris: set db_exec_path por oracle-guard-original en lugar de oracle
     - Para Oracle en AIX: set db_exec_path por oracle-guard-instrumented en lugar de oracle
   - Cambie los archivos y directorios a los que se hace referencia en las definiciones de IE de modo que sean relativos al directorio raíz de la WPAR y no a la partición global. (El orden de IE, la serie tap_identifier, etc, deben ser idénticos en todos los archivos guard_tap.ini).
8. Reinicie S-TAP.
9. Para Solaris, verifique el enlace guard_ktap y los permisos sobre cada subzona. Esto se debe realizar como **root** desde la zona global/maestra.
   a. Vaya al directorio del dispositivo de la subzona, por ejemplo: `cd /export/home2/zones/iris3/dev`
   b. Verifique que el dispositivo KTAP existe (si no es así, significa que se ha producido un problema con la instalación en 2): `ls -l ktap_*`
   c. Verifique que existe el enlace simbólico guard_ktap: `ls -l guard_ktap`
   d. Si no existe, cree uno. (Nota: ktap_xxxxx es el dispositivo que se acaba de listar): `ln -fs ktap_xxxx guard_ktap`

      Por ejemplo:

      ```
      -bash-3.00# ln -fs ktap_83164_0 guard_ktap
      -bash-3.00# ln -fs ktap_83164_1 guard_ktap1
      -bash-3.00# ln -fs ktap_83164_2 guard_ktap2
      -bash-3.00# ln -fs ktap_83164_3 guard_ktap3
      -bash-3.00# ln -fs ktap_83164_4 guard_ktap4
      -bash-3.00# ln -fs ktap_83164_5 guard_ktap5
      ```

   e. Asegúrese de cualquier usuario pueda utilizar guard_ktap y ktap_xxxxx:

      ```
      chmod 0666 ktap_xxxxx_0
      chmod 0666 ktap_xxxxx_1
      chmod 0666 ktap_xxxxx_2
      chmod 0666 ktap_xxxxx_3
      chmod 0666 ktap_xxxxx_4
      chmod 0666 ktap_xxxxx_5
      chmod 0666 guard_ktap
      chmod 0666 guard_ktap1
      chmod 0666 guard_ktap2
      chmod 0666 guard_ktap3
      chmod 0666 guard_ktap4
      chmod 0666 guard_ktap5
      ```

   Nota: ATAP, WPAR y tráfico cifrado: con una WPAR/zona, el tráfico cifrado y el tráfico descifrado tienen diferentes IP cuando este tráfico se dirige al analizador. Por lo tanto, el db_user en WPAR/zonas no tiene sentido.
10.

Tema principal: Configuración y activación de A-TAP en entornos especiales

Desactivación y desinstalación de A-TAP en entornos de zonas y de WPAR

Acerca de esta tarea

Procedimiento

1. En cada subzona/subWPAR con A-TAP instalado/activo:
   a. Desactive (y desinstrumente si es necesario, para Oracle en AIX) todos los A-TAP mediante guardctl siguiendo los pasos de Desactivación de A-TAP.
   b. Elimine manualmente (`rm -rf`) el directorio de instalación
   c. Elimine manualmente las bibliotecas de ATAP; `find /usr/lib -type f -name 'libguard-*.so' | xargs rm -f`
   Nota: La eliminación de las bibliotecas puede dar errores que se pueden pasar por alto.
2. Desinstale STAP/KTAP con el método normal
   a. Elimine las bibliotecas: `find /usr/lib -type f -name 'libguard-*.so' | xargs rm -f o`
   b.
   c. En Solaris, elimine el dispositivo ktap para la configuración de cada zona:

      ```
      zoneadm -z <zonename> halt
      zonecfg -z <zonename>
      <zonename>> info
      ```

      Si se encuentra un dispositivo ktap, elimínelo:

```
/<zonename> remove device match=/dev/ktap_xxxx (FOR SOLARIS 10)
/<zonename> remove device match=/dev/guard_ktap (FOR SOLARIS 11)
<zonename>> verify
<zonename>> exit
zoneadm -z <zonename> boot
```

d. Elimine el archivo de dispositivo de ktap y el enlace de cada directorio de dispositivo de subzona/subWPAR, por ejemplo:

```
/export/home2/zones/iris3/dev cd /export/home2/zones/iris3/dev
rm -f ktap_xxxx guard_ktap
```

e. Si hay varios dispositivos KTAP, repita los pasos para cada dispositivo KTAP utilizando el nombre ktap_xxxx (Solaris 10) o guard_ktap_x (Solaris 11).

Tema principal: Configuración y activación de A-TAP en entornos especiales

Actualización de ATAP en entornos de zonas y WPAR

Acerca de esta tarea

Procedimiento

1. Para la zona Solaris:
   a. En la zona maestra/global, elimine el dispositivo ktap instalado anteriormente.

```
zoneadm -z <zonename> halt
zonecfg -z <zonename>
<zonename>> info
```

   b. Si se encuentra un dispositivo ktap, elimínelo.

```
/<zonename> remove device match=/dev/ktap_xxxx (for Solaris 10)
/<zonename> remove device match=/dev/guard_ktap (for Solaris 11)


<zonename>> verify
<zonename>> exit
zoneadm -z <zonename> boot
```

   c. Para las subzonas de Solaris, elimine el archivo de dispositivo ktap anterior y enlace desde el directorio de dispositivo de subzona. Vaya al directorio del dispositivo de la subzona, por ejemplo /export/home2 /zones/iris3/dev.

```
cd /export/home2/zones/iris3/dev
rm -f ktap_xxxx guard_ktap
```

2. Para la zona Solaris:
   a. En la zona maestra/global, añada el nuevo dispositivo K-TAP a la configuración de la zona:

```
zoneadm -z <zonename> halt
zonecfg -z <zonename>
<zonename>> add device

<zonename>device> set match=/dev/ktap_xxxx (for Solaris 10)
<zonename>device> set match=/dev/ktap_xxxx (for Solaris 11)

<zonename>device> end
<zonename>> verify
<zonename>> exit
zoneadm -z <zonename> boot
```

   b. Añada el enlace guard_ktap y cambie el permiso. Vaya al directorio del dispositivo de la subzona, por ejemplo: sub-zone device directory=/export/home2/zones/iris3/dev

```
cd /export/home2/zones/iris3/dev
ln -fs ktap_xxxx guard_ktap
chmod 0666 ktap_xxxx
chmod 0666 guard_ktap
```

   c. Dado que hay varios dispositivos ktap, repita los pasos declarados para Doberman para cada dispositivo ktap utilizando el nombre ktap_xxxx_x (solaris 10) o guard_ktap_x (solaris 11)
3. Para las WPAR de AIX: en wpars, cambie el permiso sobre los dispositivos ktap. Vaya al directorio del dispositivo wpars, por ejemplo: wpars device directory=/wpars/odin3/dev

```
ln -fs ktap_xxxx guard_ktap
chmod 0666 ktap_xxxx
chmod 0666 guard_ktap
```

Tema principal: Configuración y activación de A-TAP en entornos especiales

Pasos para configurar y activar A-TAP para una base de datos Teradata

Paso 1: Determinar el usuario que ejecuta gtwgateway y la vía de acceso

Por ejemplo:

su11u1x64-tera:~ # ps -ef | grep gtwgateway

teradata 5000 4608 0 Jan03 ? 00:00:05 /usr/tgtw/bin/gtwgateway

root 20128 20063 0 12:35 pts/0 00:00:00 grep gtwgateway

gtwgateway se ejecuta como el usuario teradata

Establezca el parámetro *--db-user=teradata* en guardctl

La vía de acceso a gtwgateway es /usr/tgtw/bin/gtwgateway. Este es el valor predeterminado para

el parámetro tdc_gtwgateway y como tal no es necesario especificarlo.

De lo contrario, el parámetro debería ser *--tdc_gtwgateway=/usr/tgtw/bin/gtwgateway*

Paso 2: Determinar la vía de acceso a pdemain

Por lo general, será /usr/pde/bin/pdemain

Por ejemplo:

su11u1x64-tera:~ # ps -ef | grep pdemain

root 4608 1 0 Jan03 ? 00:00:25 pdemain –debug

su11u1x64-tera:~ # ls -l /proc/4608/exe

lrwxrwxrwx 1 root tdtrusted 0 2015-01-03 01:20 /proc/4608root 20620 20063

0 12:40 pts/0 00:00:00 grep pdemain/exe ->

/opt/teradata/tdat/pde/15h.00.00.07/bin/pdemain

Se comprueban los inodes para este archivo y /usr/pde/bin/pdemain; son los mismos.

su11u1x64-tera:~ # ls -li /opt/teradata/tdat/pde/15h.00.00.07/bin/pdemain

1638875 -r-xr-xr-x 1 teradata tdtrusted 1294666 2014-01-22 01:40

/opt/teradata/tdat/pde/15h.00.00.07/bin/pdemain

su11u1x64-tera:~ # ls -li /usr/pde/bin/pdemain

1638875 -r-xr-xr-x 1 teradata tdtrusted 1294666 2014-01-22 01:40

/usr/pde/bin/pdemain

Puesto que los inodes son los mismos y el valor predeterminado para *--db-home=/usr/pde*, en este caso no es necesario especificar el parámetro. De lo contrario, puede especificar --db-home=/opt/teradata/tdat/pde/15h.00.00.07 o --db-home=/usr/pde ya que bin/pdemain en ambas vías de acceso es el mismo archivo de enlace fijo en este caso.

Paso 3: Detener la instancia de Teradata

Por ejemplo:

su11u1x64-tera:~ # /etc/init.d/tgtw stop

tgtw Shutdown complete

su11u1x64-tera:~ # /etc/init.d/tpa stop

PDE stopped for TPA shutdown

Paso 4: Autorizar al usuario de la BD al grupo de Guardium

Por ejemplo:

/usr/local/guardium/guard_stap/guardctl --db-instance=teradata authorize-user

Paso 5: Almacenar la configuración de A-TAP utilizando los parámetros determinados en los pasos 1 y 2.

Por ejemplo:

/usr/local/guardium/guard_stap/guardctl --db-instance=teradata

--tdc_gtwgateway=/usr/tgtw/bin/gtwgateway --db-type=teradata

--db-home=/opt/teradata/tdat/pde/15h.00.00.07 --db-user=teradata store-conf

Paso 6: Activar A-TAP

Por ejemplo:

/usr/local/guardium/guard_stap/guardctl --db-instance=teradata activate

Paso 7: Reiniciar la instancia de Teradata

Por ejemplo:

su11u1x64-tera:~ # /etc/init.d/tpa start

Teradata Database Initiator service is starting...

Teradata Database Initiator service started successfully.

su11u1x64-tera:~ # /etc/init.d/tgtw start

tgtw Startup complete

Tema principal: Configuración y activación de A-TAP en entornos especiales

Configuración de Oracle para A-TAP

Procedimiento de A-TAP cuando se trabaja con instalaciones de parches de Oracle

Los parches de Oracle pueden invocar relink y sustituirán el ejecutable de Oracle, haciendo que el A-TAP deje de funcionar.

El procedimiento correcto es:

1. Asegúrese de que todas las instancias de A-TAP estén desactivadas
2. Aplique el parche o parches de Oracle.
3. Active A-TAP

Sin embargo, en el caso de que A-TAP no se haya desactivado correctamente antes de la instalación de los parches de Oracle, NO intente desactivarlo después de la instalación de los parches. En su lugar, siga estos pasos:

1. Compruebe si el A-TAP está en estado correcto.

```
grep guardium $ORACLE_HOME/bin/oracle >& /dev/null && echo "ATAP IS OK"
```

   a. Si se muestra `ATAP IS OK`, significa que el A-TAP sigue activo y no es necesario hacer nada.
   b. Si NO se muestra `ATAP IS OK`, elimine $ORACLE_HOME/bin/oracle-guard y active el A-TAP.

En caso de que todo lo demás falle:

- Elimine $ORACLE_HOME/bin/oracle-guard
- Ejecute relink all

Problemas y soluciones de A-TAP asociados a permisos de Oracle

Pueden producirse diversos problemas relacionados con permisos de usuario y de grupo.

- En el acceso 'BEQUEATH' desde un usuario que no sea el que ha instalado la base de datos, los permisos se tienen que definir manualmente:
  - Añada el usuario ejecutando sqlplus sobre el grupo 'guardium'
  - abra los permisos de lectura 'chmod a+rx' en los dos directorios siguientes:

    ```
    /usr/local/guardium/xxx/etc/guard
    /usr/local/guardium/xxx/etc/guard/executor
    ```

  - asegúrese de que los bits SUID y SGID estén en ${ORACLE_HOME}/bin/oracle.
    - Si no es así, ejecute el mandato chmod ug+s ${ORACLE_HOME}/bin/oracle')
- Si A-TAP no es miembro del grupo guardium, no podrá abrir el dispositivo K-Tap y verá el siguiente mensaje de syslog; indica : `ATAP [UID= GID= EUID= EGID=] al abrir ktap '' [OWNER UID= GID= PERMS=]: Permiso denegado.`
- Si el UID o el EUID no son miembros de GID del grupo OWNER, la razón por la que se ha denegado el permiso es que el usuario que coincide con el UID o el EUID no pertenece al grupo que coincide con el GID OWNER.
- Para hacerlo más fácil, sin tener que manejar las sintaxis de los distintos sistemas operativos para añadir usuarios y grupos al inhabilitar la adición automática al grupo Guardium, hay dos mandatos disponibles en guardctl que se pueden utilizar independientemente del método que se utilice para activar ATAP (es decir, guardctl) o guard_tap.ini):
  - #/path/to/guardium/bin/guardctl is-user-authorized
  - #/path/to/guardium/bin/guardctl authorize-user ...

Nota: El grupo Guardium se puede eliminar en la mayoría de los sistemas operativos con groupdel guardium. Sin embargo, después de la eliminación, sólo el parámetro guard_ktap_loader puede volverlo a crear correctamente y cambiar los permisos de dispositivo de K-TAP.
Tema principal: Configuración y activación de A-TAP en entornos especiales

Resolución de problemas de configuración de A-TAP

Esta sección contiene un resumen de los errores comunes que se realizan durante las configuraciones de A-TAP, sus síntomas y cómo evitarlos.

Tabla 1. Errores comunes de Oracle

Síntomas	Error	Plataforma	Mensaje o mensajes de error	Cómo evitarlo
El mandato de activación falla.	Parámetro db_home erróneo	Todas		Especifique siempre el valor de $ORACLE_HOME como nombre de db_home.
El mandato de activación falla.	El usuario OS ha iniciado una sesión	Todas		Asegúrese siempre de que el usuario OS no haya iniciado sesión. Utilice el mandato w para ver los usuarios que han iniciado una sesión.
La base de datos no se inicia.	Nombre de instancia incorrecto	Todas	No se ha podido ejecutar oracleon1jumbo-guard: no existe dicho archivo o directorio: no existe dicho archivo o directorio ERROR: ORA-12547: TNS:lost contact	Especifique siempre el valor de $ORACLE_SID como nombre de db_instance.

Síntomas	Error	Plataforma	Mensaje o mensajes de error	Cómo evitarlo
El tráfico no se registra.	Falta db_version o es incorrecto	AIX		Especifique siempre una versión numérica (por ejemplo, 10.2 o 9.2). El número de versión solo puede tener un dígito después del punto decimal.
No se puede activar.	Falta Oracle-guard-instrumented	AIX	Falta Oracle-guard-instrumented.	Primero se debe ejecutar el mandato instrument para crear un ejecutable de Oracle instrumentado reenlazado
error durante la activación de ATAP, el usuario debe limpiar los archivos de oracle y volverlo a intentar	Espacio de disco insuficiente, se sale de la instalación		Se ha encontrado un módulo coincidente - recibe soporte de /ngs/lpp/guardium/modules/ATAP/current/files/lib/libguard-atap-oraclesta tic-any Probando espacio de disco... cp : 0653-447 Se ha solicitado escribir 131072 bytes, pero solo se han escrito 126976. Espacio de disco insuficiente - suprima algunos archivos e inténtelo de nuevo.	change db_space=8 to db_space=1
El registro de guard_stap muestra que guard-atap-ctl ha fallado	GIM_ROOT_DIR no está establecido en la vía de acceso absoluta a los módulos, por ejemplo /usr/local/guardium/modules			Cuando se activa A-TAP a través del archivo guard_tap.ini, encryption=1 falla de forma silenciosa. Esto resulta especialmente importante cuando se ejecuta guard_stap manualmente - asegúrese de haber definido esta variable de entorno al ejecutar guard_stap.

Tabla 2. Errores comunes de DB2

Síntomas	Error	Plataforma	Mensaje o mensajes de error	Cómo evitarlo
El tráfico no se registra.	Falta el parámetro db2_* o es incorrecto	Linux		Vea Cómo determinar los parámetros de DB2

Tabla 3. Errores comunes de Informix

Síntomas	Error	Plataforma	Mensaje o mensajes de error	Cómo evitarlo
El tráfico no se registra correctamente.	Falta db_version o es incorrecto	Linux		Especifique siempre una versión numérica (por ejemplo, 7 u 11).

Tema principal: Gestión de A-TAP

Tee

Tee ha quedado en desuso y se encuentra aquí sólo como referencia.

Preparación para que los clientes locales de DB2 de UNIX utilicen Tee

Este tema no se aplica si se va a utilizar el mecanismo de K-TAP para supervisar conexiones locales.

Tee es un mecanismo de recopilación de datos no basado en kernel que se puede utilizar como una alternativa a K-TAP y, como tal, requiere que los clientes se conecten explícitamente a Tee.

No lleve a cabo este procedimiento hasta que el S-TAP se haya instalado en el servidor de DB2 y esté preparado para iniciar la recopilación de datos. Para que los clientes locales de DB2 utilicen Tee, deberá crear un alias de base de datos denominado tee y los clientes deberán cambiar su secuencia de inicio de sesión para iniciar la sesión en tee (en lugar de en el servidor de DB2).

1. Inicie la sesión en el sistema del servidor de base de datos utilizando la cuenta administrativa.
2. Localice la entrada en el archivo /etc/services correspondiente al nombre de nodo que utilizan los clientes para conectarse a la base de datos. Cada entrada de este archivo tiene el siguiente formato:

   ```
   nombre_nodo número_puerto/protocolo [alias]
   Por ejemplo: db2inst1     50000/ tcp     # Puerto de servicio de conexión de DB2
   ```

   Nota: Anote el nombre de nodo (db2inst1, en este ejemplo) y el número de puerto (50000). Cuando configure el motor de inspección, este es el número de puerto que deberá especificar como puerto real de Tee.
3. Seleccione un número de puerto no utilizado comprendido entre 1025 y 65535 para que lo use el S-TAP. Busque en el archivo /etc/services el número de puerto seleccionado para asegurarse de que no se utiliza. Cuando configure el motor de inspección, este es el número de puerto que especificará como puerto de escucha de Tee.
4. Especifique el mandato db2 para iniciar la interfaz de línea de mandatos de db2. para ejecutar este mandato, es posible que tenga que añadir el mandato a $PATH o que deba conmutar usuarios a un usuario de db2 en el sistema.
5. Escriba el mandato list node directory para obtener una lista de todos los nodos definidos. A continuación se muestra un ejemplo muy sencillo:

   ```
   db2 => list node directory
   Node Directory
   Number of entries in the directory = 2
   Node 1 entry:
   ```

```
 Node name                      = GACCTEST
 Comment                        =
 Directory entry type           = LOCAL
 Protocol                       = TCPIP
 Hostname                       = merlin
Service name                    = 50000
Node 2 entry:
 Node name                      = LOCGOOSE
 Comment                        =
 Directory entry type           = LOCAL
 Protocol                       = LOCAL
 Instance name                  = db2inst1
```

Nota: La entrada /etc/services que hemos examinado anteriormente relaciona el nombre de instancia db2inst1 con el nombre de servicio 50000.

6. Utilice el mandato catalog para crear un nodo en el servidor local para el puerto que se va a asignar como el puerto de escucha de Tee. Por ejemplo, para definir un nodo denominado localtee para el puerto 12344 en el servidor denominado goose, deberíamos escribir el mandato siguiente:

```
db2 => catalog tcpip node localtee remote goose server 12344
DB20000I  The CATALOG TCPIP NODE command completed successfully.
DB21056W  Directory changes may not be effective until the directory cache is refreshed.
```

7. Escriba el mandato terminate para actualizar el directorio. (Se cerrará el programa de utilidad de db2).

```
db2 => terminate
DB20000I  The TERMINATE command completed successfully.
```

8. Reinicie el programa de utilidad de db2 utilizando el mandato db2 y a continuación vuelva a escribir el mandato list node directory para verificar que el nodo nuevo se ha definido correctamente. Continuando con nuestro ejemplo sencillo, el nuevo nodo aparece ahora en la lista:

```
db2 => list node directory
Node Directory
 Number of entries in the directory = 3
Node 1 entry:
 Node name                      = GACCTEST
 Comment                        =
 Directory entry type           = LOCAL
 Protocol                       = TCPIP
 Hostname                       = merlin
 Service name                   = 50000
Node 2 entry:
 Node name                      = LOCALTEE
 Comment                        =
 Directory entry type           = LOCAL
 Protocol                       = TCPIP
 Hostname                       = goose
 Service name                   = 12344
Node 3 entry:
 Node name                      = LOCGOOSE
 Comment                        =
 Directory entry type           = LOCAL
 Protocol                       = LOCAL
 Instance name                  = db2inst1
```

9. Configure un alias de base de datos denominado tee para la base de datos. En nuestro ejemplo, utilizaremos una base de datos denominada SAMPLE (sustituya este valor por el nombre de su base de datos):

```
db2 => catalog database SAMPLE as tee at node localtee
DB20000I  The CATALOG DATABASE command completed successfully.
DB21056W  Directory changes may not be effective until the directory cache is
refreshed.
```

10. Escriba el mandato terminate para actualizar el directorio. (Se cerrará el programa de utilidad de db2).

```
db2 => terminate
DB20000I  The TERMINATE command completed successfully.
```

11. Reinicie el programa de utilidad de db2 utilizando el mandato db2 y a continuación escriba el mandato list database directory para verificar que el alias de la base de datos de tee se ha definido correctamente. Continuando con nuestro ejemplo sencillo, la nueva base de datos debe aparecer en la lista de bases de datos (sólo se muestra una lista parcial):

```
db2 => list database directory
System Database Directory
Number of entries in the directory = 6
Database 1 entry:
...
Database 3 entry:
 Database alias                       = DN0GOOSE
 Database name                        = SAMPLE
 Node name                            = DN0GOOSE
 Database release level               = a.00
 Comment                              =
 Directory entry type                 = Remote
 Catalog database partition number    = -1
Database 4 entry:
...
Database 5 entry:
 Database alias                       = TEE
 Database name                        = SAMPLE
 Node name                            = LOCALTEE
 Database release level               = a.00
 Comment                              =
 Directory entry type                 = Remote
 Catalog database partition number    = -1
```

12. Escriba el mandato quit para cerrar el programa de utilidad de DB2:

```
db2 => quit
```

    No cierre todavía la sesión del sistema del servidor de base de datos. Después de configurar un motor de inspección, deberá especificar uno o varios mandatos SQL utilizando el programa de utilidad SQL de línea de mandatos DB2 para verificar la conexión de alias.
13. Cuando esté preparado para iniciar la recopilación de datos, defina un motor de inspección de DB2 para que escuche en el puerto de escucha de Tee (12344 en el ejemplo) y reenvíe los mensajes al puerto real de Tee (50000 en el ejemplo). Asegúrese de establecer todas las demás propiedades necesarias para un motor de inspección de DB2, tal como se describe en otra sección.
14. Utilice la línea de mandatos de DB2 para verificar que la conexión de base de datos a través del proceso Tee local funciona correctamente. Inicie una sesión en la base de datos desde la línea de mandatos utilizando un mandato como el siguiente (donde sample es la base de datos o algún nombre de catálogo de Tee, db2inst1 es el nombre de usuario, passwd es la contraseña y tee es el alias de la base de datos):

```
$ db2 connect to sample user db2inst1 using passwd
   Database Connection Information
 Database server        = DB2/LINUXX8664 9.7.0
 SQL authorization ID   = DB2INST1
 Local database alias   = SAMPLE
```

15. Especifique un mandato que sepa que creará una excepción de SQL (por ejemplo, select * from my_error) y, a continuación, salga de la sesión.
16. Inicie una sesión en un portal de usuario en el sistema Guardium, vaya al separador Informes y Alertas - Plantillas de informes - Excepciones y seleccione el informe Errores de SQL. Debería ser capaz de localizar el error de SQL casi al principio del informe y, por lo tanto, verificar que Tee está viendo el tráfico de Informix.
17. Ahora modifique todos los inicios de sesión del cliente para que se inicie la sesión en el alias de Tee (en lugar de en el servidor de DB2).

Preparación para que los clientes locales de Informix de UNIX utilicen Tee

Este tema no se aplica si se va a utilizar el mecanismo K-Tap para supervisar las conexiones locales. Tee es un mecanismo de recopilación de datos no basado en kernel que se puede utilizar como una alternativa a K-TAP y, como tal, requiere que los clientes se conecten explícitamente a Tee.

No lleve a cabo este procedimiento hasta que el S-TAP se haya instalado en el servidor de Informix y esté preparado para iniciar la recopilación de datos. Para que los clientes de Informix locales utilicen Tee, deberá crear un nombre de servicio staptcp en el archivo /etc/services, crear un archivo stap_sqlhosts y modificar varias variables de entorno de forma que los clientes de Informix locales se conecten al puerto de Tee en lugar de al servidor Informix.

1. Localice el archivo sqlhosts. El nombre de archivo predeterminado es sqlhosts y, de forma predeterminada, se encuentra en el directorio $INFORMIXDIR/etc/. El nombre de archivo y la ubicación predeterminados se pueden modificar mediante la variable de entorno INFORMIXSQLHOSTS, que, cuando está presente, define el nombre completo de la vía de acceso del archivo.
2. Haga una copia del archivo sqlhosts y llámela stap_sqlhosts. Luego modificará la copia. No modifique el archivo sqlhosts original. No hay requisitos de denominación para el archivo. Utilizaremos el nombre stap_sqlhosts en el resto de esta sección.
3. Abra el archivo stap_sqlhosts en un editor de texto.
4. Localice la entrada que utilizan los clientes locales para conectar con la base de datos. Cada entrada contiene varios parámetros posicionales, en el formato siguiente:

```
nombreservidorbd tipored nombrehost nombreservicio [opciones]

Por ejemplo:
jumboinformix onsoctcp jumbo    nettcp
```

5. Fíjese en el valor del parámetro servicename (nettcp en este ejemplo). Identifica un nombre de servicio que se correlaciona con un número de puerto para este servidor de base de datos, en el archivo services. Utilizará este nombre más adelante para localizar una entrada en dicho archivo.
6. Sustituya el nombre de servicio especificado por un nuevo nombre de servicio para S-TAP. No hay requisitos de denominación. En este ejemplo utilizaremos staptcp. Siguiendo con el ejemplo, la entrada se modificaría de la siguiente manera:

```
jumboinformix onsoctcp jumbo    staptcp
```

7. Guarde el archivo stap_sqlhosts.
8. Localice el archivo services. De forma predeterminada, está en el directorio /etc, pero si se utiliza el Servicio de información de red (NIS), debe editar el archivo services en el servidor NIS.
9. Haga una copia de seguridad del archivo y abra el original para editarlo.
10. Localice la entrada en el archivo services para el nombre de servicio que ha sustituido en el archivo stap_sqlhosts. Cada entrada de este archivo tiene el siguiente formato:

```
nombreservicio número_puerto/protocolo [alias]
En nuestro archivo de servicios de ejemplo, la entrada nettcp está definida de la siguiente manera: nettcp      1400/tcp
```

    Nota: Preste atención al número de puerto (1400, en el ejemplo). Cuando configure el motor de inspección, este es el número de puerto que deberá especificar como puerto real de Tee.
11. Seleccione un número de puerto no utilizado comprendido entre 1025 y 65535 para que lo use el S-TAP. Busque en el archivo services el número de puerto seleccionado para asegurarse de que no se utiliza. En nuestro ejemplo, utilizaremos 12344. Cuando configure el motor de inspección, este es el número de puerto que especificará como puerto de escucha de Tee.
12. Añada una línea al archivo services para el puerto de escucha de S-TAP, staptcp en el ejemplo:

```
staptcp     12344/tcp
```

13. Guarde el archivo services.
14. Establezca la variable de entorno INFORMIXSQLHOSTS, para especificar el nombre completo de la vía de acceso para la versión clonada del archivo sqlhosts que ha creado anteriormente. Por ejemplo:

```
setenv INFORMIXSQLHOSTS $INFORMIXDIR/etc/stap_sqlhosts
```

15. Cuando esté preparado para iniciar la recopilación de datos, defina un motor de inspección de Informix para que escuche en el puerto de escucha de Tee (12344 en el ejemplo) y reenvíe los mensajes al puerto real de Tee (1400 en el ejemplo).
16. Puede utilizar el mandato dbaccess para verificar que S-TAP está viendo las solicitudes SQL del cliente. Para utilizar dbaccess, se deben definir correctamente tres variables de entorno: INFORMIXDIR, INFORMIXSERVER e INFORMIXSQLHOSTS. Verifique que estas variables están establecidas correctamente utilizando el mandato siguiente:

```
-bash-3.00# env | grep INFO
INFORMIXDIR=/data/informix
```

```
INFORMIXSERVER=jumboinformix
INFORMIXSQLHOSTS=/data/informix/etc/stap_sqlhosts
```

INFORMIXSERVER identifica el servidor de base de datos al que se está intentando conectar (jumboinformix en este ejemplo).

INFORMIXSQLHOSTS identifica el archivo sqlhosts utilizado para resolver las conexiones con jumboinformix. Durante esta resolución, será una conexión TCP o memoria compartida. En nuestra definición anterior, es una conexión TCP con el nombre de servicio staptcp. Se conectará al puerto TCP correcto, 12344, que se resuelve en el archivo /etc/services.

17. Escriba el mandato dbaccess.
18. Vaya a conexión - conectar - Seleccionar servidor de base de datos y seleccione el nombre de servidor de base de datos (jumboinformix en nuestro ejemplo).
19. Cuando se le solicite, especifique un nombre de usuario y una contraseña de base de datos apropiados.
20. Salga de la parte de conexión de la configuración y seleccione Lenguaje de consulta - seleccionar base de datos.
21. Seleccione Nuevo y especifique un mandato de SQL, por ejemplo: select * from my_error.
22. Inicie una sesión en un portal de usuario en el sistema Guardium, vaya al separador Informes y Alertas - Plantillas de informes - Excepciones y seleccione el informe Errores de SQL. Debería ser capaz de localizar el error de SQL casi al principio del informe y, por lo tanto, verificar que Tee está viendo el tráfico de Informix.

Preparación para que los clientes locales de Oracle de UNIX utilicen Tee

Este tema no se aplica si se va a utilizar el mecanismo K-Tap para supervisar las conexiones locales. Tee es un mecanismo de recopilación de datos no basado en kernel que se puede utilizar como una alternativa a K-Tap y, como tal, requiere que los clientes se conecten explícitamente a Tee.

No lleve a cabo este procedimiento hasta que el S-TAP se haya instalado en el servidor Oracle y esté preparado para iniciar la recopilación de datos. Siga el procedimiento siguiente en el que se describe cómo modificar el archivo tnsnames.ora, que correlaciona alias de servicio con puertos. No modifique este archivo hasta que el S-TAP se haya instalado y esté preparado para iniciar la recopilación de datos.

1. Haga una copia de seguridad del archivo tnsnames.ora, que se encuentra en el directorio $ORACLE_HOME/network/admin.
2. Abra el archivo tnsnames.ora para editarlo en un programa editor de texto.
3. Localice la entrada en este archivo para el alias de servicio utilizado para acceder a la base de datos. A continuación se muestra una entrada denominada EAGLE10 en el host de EAGLE:

```
EAGLE10 =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = eagle)(PORT = 1521)))
    (CONNECT_DATA = (SERVICE_NAME = GUARD10))
   )
```

4. Anote el número de puerto utilizado (1521, en este ejemplo). Cuando configure el motor de inspección, este es el número de puerto que deberá especificar como puerto real de Tee. No modifique la entrada hasta que haya verificado que el S-TAP se ha configurado correctamente.
5. Seleccione un número de puerto no utilizado comprendido entre 1025 y 65535 para que lo use el S-TAP. Busque en el archivo el número de puerto seleccionado para asegurarse de que no se utiliza. En nuestro ejemplo, utilizaremos 12344. Cuando configure el motor de inspección, este es el número de puerto que especificará como puerto de escucha de Tee.
6. Cree una entrada duplicada para el servicio copiando y pegando la entrada y haciendo los cambios resaltados. Llamaremos LOCALTEE a nuestro duplicado:

```
LOCALTEE =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = eagle)(PORT = 12344)))
    (CONNECT_DATA = (SERVICE_NAME = GUARD10))
   )
```

7. Guarde el archivo tnsnames.ora.
8. Cuando esté preparado para iniciar la recopilación de datos, defina un motor de inspección de Oracle para que escuche en el puerto de escucha de Tee (12344 en el ejemplo) y reenvíe los mensajes al puerto real de Tee (1521 en el ejemplo).
9. Inicie una sesión localmente en el servidor de base de datos, utilizando sqlplus para verificar que el S-TAP se ha configurado correctamente; verá un acceso local. Por ejemplo:

```
# sqlplus scott/tiger@LOCALTEE
```

Donde scott es el nombre de usuario de la base de datos, tiger es la contraseña y LOCALTEE identifica el servicio.

10. Escriba un mandato SQL no válido para crear una excepción de SQL que sea fácil de encontrar. Por ejemplo: select * from my_mistake
11. Inicie una sesión en un portal de usuario en el sistema Guardium, vaya al separador Informes y Alertas - Plantillas de informes - Excepciones y seleccione el informe Errores de SQL. Debería ser capaz de localizar el error de SQL casi al principio del informe y, por lo tanto, verificar que Tee está viendo el tráfico local de Oracle.
12. Vuelva a abrir el archivo tnsnames.ora y sustituya el número de puerto del servicio de base de datos por el número seleccionado. Siguiendo con nuestro ejemplo, la entrada EAGLE10 se actualizaría de la siguiente manera:

```
EAGLE10 =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = eagle)(PORT = 12344)))
    (CONNECT_DATA = (SERVICE_NAME = GUARD10))
   )
```

13. Guarde el archivo tnsnames.ora. Todos los clientes locales que se conecten a EAGLE10 se conectarán ahora al puerto 12344 (el puerto de escucha de Tee) en lugar de al puerto real de la base de datos (el puerto real de Tee).

Preparación para que los clientes locales de Sybase de UNIX utilicen Tee

Este tema no se aplica si se va a utilizar el mecanismo K-Tap para supervisar las conexiones locales. Tee es un mecanismo de recopilación de datos no basado en kernel que se puede utilizar como una alternativa a K-Tap y, como tal, requiere que los clientes se conecten explícitamente a Tee.

Siga estos pasos para modificar el archivo de interfaz local, que correlaciona servidores con puertos. No modifique este archivo hasta que el S-TAP se haya instalado y esté preparado para iniciar la recopilación de datos.

1. Haga una copia de seguridad del archivo de interfaz, que se encuentra en el directorio $SYBASE/.

2. Abra el archivo de interfaz para editarlo en un programa editor de texto.
3. Localice la entrada en este archivo cuyo nombre coincida con el nombre del servidor de Sybase. Por ejemplo, un servidor denominado parrot se puede definir de la siguiente manera:

```
parrot
    master tcp ether parrot 4100
    query tcp ether PARROT 4100
```

4. Anote el número de puerto (4100, en el ejemplo). Cuando configure el motor de inspección, este es el número de puerto que deberá especificar como puerto real de Tee.
5. Seleccione un número de puerto no utilizado comprendido entre 1025 y 65535 para que lo use el S-TAP. Busque en el archivo el número de puerto seleccionado para asegurarse de que no se utiliza. En nuestro ejemplo, utilizaremos 12344. Cuando configure el motor de inspección, este es el número de puerto que especificará como puerto de escucha de Tee.
6. Sustituya el número de puerto por el número seleccionado. Por ejemplo:

```
parrot
    master tcp ether parrot 12344
    query tcp ether PARROT 12344
```

7. Guarde el archivo de interfaz.
8. Cuando esté preparado para iniciar la recopilación de datos, defina un motor de inspección de Sybase para que escuche en el puerto de escucha de Tee (12344 en el ejemplo) y reenvíe los mensajes al puerto real de Tee (4100 en el ejemplo).

Conmutación de Tee a K-Tap

Siga los pasos siguientes para conmutar de Tee a K-Tap sin desinstalar ni reinstalar. Esta condición puede producirse después de una carga incorrecta de K-Tap.

1. Inhabilite S-TAP. Consulte el apartado sobre cómo detener S-TAP de UNIX para obtener más información.
2. Comente las líneas guard_tee y guard_hnt en inittab, o realice el cambio adecuado para Red Hat 6 que no utiliza inittab
3. Ejecute 'init q' o equivalente de Red Hat; como alternativa, simplemente termine los trabajos de Tee y Hunter
4. Edite guard_tap.ini y cambie ktap_installed por 1 y tee_installed por 0
5. Ejecute el mandato 'guard_ktap_loader install'
   Nota: Para Linux, establezca primero la variable de entorno NI_ALLOW_MODULE_COMBOS="Y"
   Ejemplo de Linux:

```
NI_ALLOW_MODULE_COMBOS="Y"
/usr/local/guardium/guard_stap/ktap/current/guard_ktap_loader install
```

   Ejemplo que no es de Linux:

```
/usr/local/guardium/guard_stap/ktap/current/guard_ktap_loader install
```

6. Ejecute el mandato 'guard_ktap_loader start'

```
Ejemplo: /usr/local/guardium/guard_stap/ktap/current/guard_ktap_loader start
```

7. Vuelva a habilitar S-TAP. Consulte el apartado sobre cómo reiniciar S-TAP de UNIX para obtener más información.

Tema principal: S-TAPs y otros agentes

Configuración de S-TAP desde la GUI

Después de instalar un agente de S-TAP en un servidor de base de datos, la configuración de S-TAP se puede realizar desde la GUI.

Control de S-TAP - Realice una configuración de S-TAP

Para realizar cambios en la configuración de S-TAP, debe haber iniciado sesión en el sistema Guardium que sea el host activo del S-TAP. Sólo puede editar una configuración de S-TAP desde su host activo. Algunos cambios de configuración requieren que el agente de S-TAP se reinicie manualmente.

Pulse Gestionar > Supervisión de actividad > Control de A-TAP para abrir Control de S-TAP.

Si no hay ninguna sección Taps locales, primero debe configurar el sistema Guardium para gestionar los agentes de S-TAP. Consulte Configuración del sistema Guardium para gestionar S-TAP para obtener más información.

Localice el S-TAP que desea configurar en la columna Host de S-TAP mirando su dirección IP o el nombre de host simbólico del servidor de base de datos en el que está instalado. Cada S-TAP tiene sus propios controles, que se muestran en la tabla siguiente.

Control	Descripción
Suprimir	Pulse Suprimir para eliminar un S-TAP. No puede eliminar de la lista un S-TAP activo. Si se pulsa suprimir, no se impide que el S-TAP envíe información ni se elimina el host de Guardium de la lista de hosts almacenados en el archivo de configuración del S-TAP. La supresión de S-TAP resulta útil para limpiar la pantalla cuando se sabe que un S-TAP ha pasado a estar inactivo, o cuando la unidad de Guardium ya no aparece en la lista de como host en el archivo de configuración de S-TAP. En cualquiera de estos dos casos, el S-TAP se visualiza de forma indefinida con el estado Fuera de línea.
Renovar	Pulse Renovar para captar una copia de la configuración más reciente de S-TAP del agente.
Enviar	Pulse Enviar para reiniciar, reinicializar el almacenamiento intermedio, ejecutar diagnósticos o cambiar los parámetros de registro de S-TAP o K-TAP.
Registro de S-TAP	Parámetros de registro de S-TAP: Nivel de depuración:

	0 - solo información de errores críticos 1 - todo lo del nivel anterior incluido, más información repetible de errores no críticos 2 - todo lo del nivel anterior incluido, más información sobre datos perdidos (suspendido desde versión 4.03 y posteriores) 3 - todo lo del nivel anterior incluido, más una breve información sobre los paquetes enviados a un recopilador de Guardium 4 - todo los del nivel anterior incluido, más registro de rastreo local 5 - todo los del nivel anterior incluido, más registro de rastreo de red 6 - todo lo del nivel anterior incluido, más registro de recepción de latido 7 - todo lo del nivel anterior incluido, más información diversa sobre depuración Segundos de duración de depuración: duración de la sesión de depuración (en segundos)
Reinicializar almacenamiento intermedio	Envía un mensaje al S-TAP que solicita que reinicialice su almacenamiento intermedio y se vuelva a iniciar
Registro de K-TAP	Escriba el Nombre de función y la Segundos de duración de depuración
Ejecutar diagnósticos	Ejecuta diagnósticos en el S-TAP Para Windows, los archivos de depuración se encuentran en STAP_HOME/TempSnapshot/ con un nombre de archivo como debug_Feb_25_2009_10_59_59.txt. Para UNIX, los archivos de depuración están en el directorio /tmp con el nombre de archivo /tmp/guard_stap.stderr.txt.
Editar	Editar solo está habilitado si el sistema Guardium es el host activo del S-TAP. Nota: En un entorno de equilibrador de carga de IP, la edición de la configuración de S-TAP se puede inhabilitar.
Registro de información	Muestra el registro de sucesos de S-TAP
Host de S-TAP	La dirección IP o el nombre de host
Estado	Estado del S-TAP Se iluminará una de estas tres luces: **Verde** (En línea) – El S-TAP funciona con normalidad. **Roja** (Fuera de línea) – El S-TAP no responde. **Amarillo** (No sincronizado) – Se han enviado cambios de configuración al S-TAP, pero el S-TAP aún no ha confirmado que los cambios se hayan aplicado. Si la luz permanece amarilla durante un largo periodo de tiempo, puede dar por supuesto que el S-TAP no ha aceptado la nueva configuración. Cuando esto sucede, el S-TAP intenta reiniciarse utilizando la última configuración correcta. Cuando se produzca un error, puede abrir el panel Sucesos de S-TAP en una ventana aparte pulsando Mostrar registro. En muchos casos, el registro de sucesos contiene mensajes de error que indican qué ha fallado con la nueva configuración. Para volver a cargar la última configuración correcta desde el host de S-TAP, pulse Renovar información de S-TAP. Nota: Si tiene problemas para determinar el color de la luz, mantenga el puntero del ratón sobre el conjunto de luces para ver el estado actual del S-TAP (Fuera de línea, No sincronizado o En línea).
Última respuesta	Fecha y hora de la última respuesta procedente del S-TAP

Efectúe los cambios que desee y verifique que el Indicador de estado sea verde. Si el Indicador de estado no es verde, significa que el sistema Guardium y S-TAP no están conectados.

1. Verifique que el indicador de estado sea verde . Si no es así, significa que el sistema Guardium y el S-TAP no están conectados.
2. Pulse el botón (Editar) correspondiente a dicho S-TAP. Si el botón Editar no está activo, significa que este sistema Guardium no es el host activo para este S-TAP. Debe iniciar la sesión en el host activo para que este S-TAP realice los cambios.
3. Expanda y realice modificaciones en cualquiera de las secciones siguientes de la configuración de S-TAP. Generalmente, la única tarea adicional en este punto consiste en definir uno o varios motores de inspección. (Un motor de inspección identifica un conjunto de conexiones de base de datos que supervisar). Pulse cualquiera de estas secciones para obtener una descripción detallada de su uso.
   - Control de S-TAP - Detalles
   - Control de S-TAP - Hunter
   - Control de S-TAP - Auditoría de cambios
   - Control de S-TAP - Identificación del usuario del servidor de aplicaciones
   - Control de S-TAP - Hosts de Guardium
   - Control de S-TAP - Motores de inspección
4. Si ha actualizado alguna información y desea guardar la nueva configuración, pulse Aplicar.
5. Vuelva a comprobar que la luz de estado del panel de control de S-TAP es verde. Si la luz de estado se ha vuelto amarilla, intente renovar la pantalla de S-TAP completa con el botón de renovación. Si la luz permanece amarilla, significa que S-TAP no se ha podido reiniciar utilizando la nueva configuración. Cuando esto sucede, S-TAP intenta reiniciarse utilizando la última configuración correcta. La configuración del panel de control de S-TAP aún contiene los cambios que ha aplicado, incluidos los errores. Para volver a cargar la última configuración correcta desde el host de S-TAP en el panel de control de S-TAP, pulse (Renovar información de S-TAP).

Control de S-TAP - Detalles

La sección de detalles del panel Control de S-TAP se aplica a los valores de configuración básicos para el agente de S-TAP.

Control	**Descripción**
Versión	La versión de S-TAP instalada
Dispositivos	Siempre en blanco para un servidor Windows. Para un servidor UNIX, cuando se utiliza KTAP (casi todos los casos actualmente), los dispositivos siempre se deben establecer en ninguno.
Equilibrio de carga	Este recuadro controla la forma en que el S-TAP informa del tráfico al sistema Guardium: • 0 = Notificar todo el tráfico a un único sistema Guardium (valor predeterminado). • 1 = Equilibrio de carga; distribuir las sesiones uniformemente entre todos los sistemas Guardium, por número de puerto de cliente (todo el tráfico correspondiente a una única sesión va al mismo sistema Guardium). • 2 = Redundancia completa; notificar todo el tráfico a todos los sistemas Guardium. • 3 = En un entorno de equilibrador de carga IP, si el sistema Guardium deja de estar activo, el equilibrador de carga IP puede volver a conectar el S-TAP a otro sistema Guardium. Nota: No es necesario establecer más de un sistema Guardium primario, ya que las máquinas primaria o secundaria tienen la misma prioridad.
Mensajes	Controla dónde se escriben los mensajes de proceso de S-TAP (no el tráfico de base de datos): • **Remoto** En el host activo de Guardium. • **Syslog** En el archivo syslog en el servidor de base de datos. Como AIX no da soporte a mensajes de syslog, los mensajes de S-TAP que normalmente irían a syslog se escriben en las siguientes ubicaciones: los registros de K-TAP van a /var/log/ktap.log; los registros de S-TAP (cuando S-TAP se encuentra en modalidad de depuración) van a stdout/stderr.
Directorio de archivos de rastreo	El directorio en el que se escriben los archivos de rastreo.
IP alternativas	Una o varias direcciones IP virtuales o alternativas utilizadas para conectar con este servidor de base de datos. Sólo se utiliza cuando el servidor tiene varias tarjetas de red con varias IP o IP virtuales. S-TAP sólo supervisa el tráfico cuando la IP de destino coincide con la IP de host S-TAP definida para este S-TAP o con una de las IP alternativas que se muestran. Por este motivo se recomienda que liste aquí todas las IP virtuales.
Memoria compartida	Sólo Windows. Controla la acción que se debe emprender cuando se detecta una conexión de memoria compartida: • **Inhabilitar** Desconectar la sesión. • **Alerta** Enviar una alerta.
Supervisor de memoria compartida	Sólo Windows. Marque los recuadros de selección para habilitar los controladores de memoria. Para mejorar el rendimiento, inhabilite los controladores que no se utilicen. **Nota:** Después de habilitar o inhabilitar cualquier controlador de memoria compartida, debe reiniciar el servicio S-TAP para que el cambio entre en vigor.
Cifrado de SQL de MS	Sólo Windows. **Nota:** Después de cambiar cualquiera de estos parámetros, debe reiniciar el servicio de S-TAP para que el cambio entre en vigor y debe reiniciar el servicio de supervisión de MSSQL. Controla el tipo de descifrado automático que se aplica al tráfico que ve S-TAP: **Ninguno** No hay descifrado automático. Se pasa por alto todo el SQL del tráfico de SSL. Se ve todo el SQL del tráfico de Kerberos, pero el nombre de usuario de la base de datos se sustituye por una serie de caracteres hexadecimales (lo hace Kerberos). **Kerberos y SSL** Descifra SSL automáticamente y correlaciona los nombres de Kerberos. Utilice esta opción si parte del tráfico que le interesa utiliza Kerberos, pero no utiliza también SSL. Si se utilizan tanto Kerberos como SSL para todo el tráfico que le interesa, utilice la opción Sólo SSL. **Sólo SSL** Descifra automáticamente el tráfico SSL. Utilice esta opción si todo el tráfico que le interesa es tráfico SSL. En este caso, aunque también se utilice la autenticación Kerberos, no tiene consecuencia, porque S-TAP obtiene toda la información que necesita antes de que se cifre el mensaje y antes de que Kerberos sustituya el nombre de usuario real de la base de datos.
Correlación de credenciales de Kerberos	Sólo Windows. Cuando se utiliza la autenticación de Kerberos, controla la forma en que S-TAP obtiene los nombres de usuario de la base de datos. Si se selecciona la opción **Sinc**, S-TAP no reenvía los mensajes al sistema Guardium hasta que resuelve el nombre de usuario real de la base de datos. Por lo tanto, en situaciones de gran volumen de mensajes, es posible que algunos mensajes se pierdan. Cuando se utiliza la opción **Asínc**, todos los mensajes se reenvían al sistema Guardium, pero las sesiones iniciales para los usuarios con nuevas incidencias de Kerberos tienen series de caracteres hexadecimales en el campo de nombre de usuario de la base de datos hasta que S-TAP resuelve el nombre de usuario de la base de datos real. **Al iniciar, síncrono** Durante el proceso de inicio, S-TAP obtiene todos los usuarios autenticados del controlador del dominio. Esto puede requerir mucho tiempo. Después de haber obtenido y presentado todos los usuarios, S-TAP inicia el envío de datos al sistema Guardium. Cuando encuentra un mensaje de un usuario que no reconoce, obtiene ese nombre de usuario de base de datos tal como se describe para A petición, síncrono. **A petición, síncrono** Cuando S-TAP encuentra un mensaje de Kerberos correspondiente a un usuario que no reconoce, S-TAP capta el nombre de usuario del controlador del dominio. No reenvía tráfico desde este usuario al sistema Guardium hasta que tiene el nombre de usuario de la base de datos real.

	A petición, asíncrono Igual que **A petición, síncrono**, excepto en que los mensajes no se retienen mientras se espera a obtener el nombre de usuario de la base de datos.
TLS	**Utilizar** Marque esta opción para utilizar una conexión TLS (cifrada). Esto se aplica tanto a los agentes de S-TAP como a los de CAS. Antes de cambiar este valor, verifique que los puertos utilizados para este propósito no estén siendo bloqueados por un cortafuegos entre el servidor y el sistema Guardium. Consulte la tabla de requisitos de puertos de Guardium en Instalación de S-TAP. **Sustitución por anomalía** Marque esta opción para indicar que, si no se puede establecer ninguna conexión TLS, se puede utilizar una conexión que no sea TLS. **Mensaje de estado activo de TCP** Si se selecciona esta opción, el S-TAP envía un mensaje de estado activo al sistema Guardium cada cinco segundos a través de la conexión TCP existente. Si se deja en blanco, el S-TAP envía mensajes de estado activo a través de TCP en respuesta a mensajes UDP procedentes del sistema Guardium. **Nota:** Sólo Windows. Después de cambiar este valor, debe reiniciar el servicio S-TAP para que el cambio entre en vigor. **Nota:** Puesto que las conexiones TLS pueden experimentar mucho tráfico y tener la sobrecarga adicional del cifrado, se pueden abrir conexiones adicionales, si reciben soporte de las CPU adicionales, mediante el parámetro connection_pool_size.
Descubrir automáticamente	Sólo en Windows, realiza el descubrimiento de bases de datos MSSQL cada vez que se inicia el S-TAP. Si se descubre una nueva base de datos MSSQL, se crea un motor de inspección y se escribe un nuevo registro en el registro de descubrimiento. El valor predeterminado es que esta opción esté desactivada.

Inhabilitación de TLS 1.0/1.1, habilitación de TLS 1.2

Para aumentar la seguridad del sistema Guardium, en Guardium release v10.1.4 los protocolos de comunicaciones TLS 1.0/1.1 se pueden inhabilitar de forma opcional.

El cliente de Guardium debe inhabilitar TLS 1.0/1.1 desde su Gestor central y/o unidad autónoma utilizando la interfaz de la línea de mandatos. Los dispositivos de Guardium del cliente, los agentes de S-TAP, los clientes de CAS y GIM deben tener versiones específicas para poder habilitar esta nueva característica.

La inhabilitación de TLS 1.1 realizará una comprobación automática para asegurarse de que las unidades gestionadas y los S-TAP tengan versiones específicas, pero no puede comprobar las versiones de cliente de CAS. Los clientes que utilicen CAS deberán asegurarse de tener la versión 10.1.4 y de que sus servidores de base de datos tengan habilitado Java 7. Si no se hace esto, no se podrán ver las conexiones de CAS con los servidores de base de datos.

Los clientes también deben asegurarse de que todas las unidades gestionadas tengan instalada la versión 10.1.4, y los clientes GIM y los S-TAP se tengan como mínimo la versión 10.1.2. Si se no cumplen todos los requisitos, no se inhabilitará TLS 1.0/1.1. La inhabilitación de TLS 1.0/1.1 dará lugar a que solo se habilite el protocolo TLS 1.2.

Pasos para inhabilitar TLS 1.0/1.1

Los usuarios de Guardium con el rol de administrador deben especificar los siguientes mandatos de GuardAPI en el indicador de la CLI. Estos mandatos son nuevos para Guardium v10.1.4.

```
grdapi get_secured_protocols_info
```

Este mandato GuardAPI mostrará una lista de los protocolos habilitados (TLS 1.0/1.1 y TLS 1.2)) e indicará si se pueden inhabilitar los protocolos en desuso. Los códigos de error mayores de 1000 indican un problema con un componente que es necesario que resuelva el administrador antes de poder inhabilitar TLS 1.0/1.1. Se visualizarán mensajes indicando el componente o componentes que no satisfacen los requisitos para inhabilitar TLS 1.0/1.1. Se generarán mensajes de aviso para las unidades gestionadas que están fuera de línea o a las que no es posible acceder. Las unidades fuera de línea se deben gestionar de forma individualizada cuando pasen a estar de nuevo en línea. Consulte local_disable_deprecated_protocols a continuación.

```
grdapi disable_deprecated_protocols
```

Este mandato GuardAPI ejecutará en primer lugar las comprobaciones de versión descritas anteriormente. Si los requisitos para la inhabilitación se cumplen, entonces este mandato cambiará los valores de configuración para cada servicio en el Gestor central, así como en todas las unidades gestionadas.

Si no se cumplen los requisitos para la inhabilitación, entonces este mandato indicará que hay habilitados protocolos en desuso que deben mantenerse habilitados hasta que no se hayan actualizado todas las unidades gestionadas y/o componentes.

Después de que se hayan realizado todos los cambios de configuración, los usuarios de Guardium con el rol de administrador deberían comprobar que las comunicaciones entre el Gestor central y las unidades gestionados son estables y que funcionan adecuadamente.

```
grdapi local_disable_deprecated_protocols
```

Para cualquier unidad gestionada que estuviera fuera de línea durante la inhabilitación de los protocolos en desuso, los usuarios de Guardium con el rol de administrador deben iniciar manualmente una sesión de línea de mandatos en la unidad gestionada y ejecutar local_disable_depreciated_protocols para realizar los cambios de configuración.

```
grdapi enable_deprecated_protocols all=true
```

Este mandato GuardAPI cambiará de nuevo a los valores de configuración antiguos y reiniciará los servicios en el Gestor central y en todas las unidades gestionadas para habilitar los protocolos en desuso. Este mandato GuardAPI se puede ejecutar con el argumento all=true desde un Gestor central para habilitar los protocolos en desuso en el Gestor central y en todas las unidades gestionadas. La ausencia del parámetro all=true habilitará los protocolos en desuso en únicamente en el dispositivo que ejecuta la GuardAPI.

Después de que se hayan realizado todos los cambios de configuración, los usuarios de Guardium con el rol de administrador deberían comprobar que las comunicaciones entre el Gestor central y las unidades gestionados son estables y que funcionan adecuadamente. Tenga en cuenta que las comunicaciones pueden ser menos seguras cuando se utiliza TLS 1.0/1.1.

Control de S-TAP - Hunter

Hunter ha quedado en desuso. Esta información solo se muestra como referencia.

El componente Hunter de S-TAP no se utiliza para servidores Windows y no se utiliza en la configuración de S-TAP de UNIX recomendada. Se utiliza opcionalmente en los S-TAP de UNIX, cuando se utiliza el mecanismo de supervisión TEE en lugar del mecanismo de supervisión de nivel de kernel recomendado.

Nota: Sólo en Solaris 11 - Si no se ha instalado inicialmente Tee, es necesario realizar una reinstalación. O bien TEE se debe instalar manualmente.
Nota: El componente Hunter no resulta visible cuando K-Tap está instalado.

Cuando se utiliza, el componente Hunter se puede configurar de modo que notifique, y opcionalmente elimine, las conexiones inesperadas que descubre en el servidor de bases de datos. Una conexión inesperada es cualquier conexión que pase por alto el mecanismo TEE.

Control	Descripción
Hunt	Identifica todos los procesos que se van a interrumpir, utilizando la sintaxis siguiente: **db_type:process [,db_type:process]** **db_type** puede ser: • DB2 • Informix • Oracle • Sybase • PostgreSQL • Teradata **process** puede ser: • **SHM** Memoria compartida • **IPv4** Internet Protocol versión 4 • **IPv6** Internet Protocol versión 6 • **FIFO** Un mecanismo de IPC de conducto con nombre • **PIPE** Un conducto IPC simple (sin nombre) • **INET** Protocolo Internet (HPUX) Estos valores no son sensibles a las mayúsculas y minúsculas y cada entrada se separa de la siguiente mediante una coma. **Ejemplo**: Para interrumpir procesos Bequeath de Oracle, que utilizan un conducto simple, debe especificar: oracle:pipe
Tiempo de inactividad	Número máximo de segundos entre la hora de inicio aleatoria de la rutina de búsqueda de procesos inesperados de Hunter. La hora de inicio es aleatoria para aumentar la dificultad de ataque mediante su ejecución en intervalos de tiempo fijos o variables. El valor recomendado para el tiempo de inactividad es el comprendido entre 60 y 300.
DB	Los tipos de base de datos que se van a notificar, en una lista separada por comas: • DB2 • Informix • Oracle • Sybase • PostgreSQL • Teradata

Control de S-TAP - Auditoría de cambios

El panel Auditoría de cambios del panel Control de S-TAP sólo se aplica al agente CAS (Configuration Auditing System). El producto CAS es un componente opcional que no está relacionado con S-TAP, pero todos los componentes de Guardium instalados en el servidor de base de datos comparten un único archivo de configuración.

Control	Descripción	
.	Punto de comprobación de tarea Punto de comprobación de cliente	Estos archivos se utilizan para el proceso de reinicio. Para cada uno de estos dos nombres de archivo, se creará una serie de archivos. Cada versión del archivo finalizará con un número de exclusividad. Los valores predeterminados de UNIX son task_checkpoint y client_checkpoint, respectivamente, y los valores predeterminados de Windows son los mismos, pero con todas las letras mayúsculas.
Periodo de punto de comprobación	El número máximo de segundos entre puntos de comprobación. El valor predeterminado es 60.	
Archivo de sustitución por anomalía	Nombre del archivo en el que se escriben los datos cuando no se puede acceder al sistema Guardium. Durante este tiempo, es posible que el archivo crezca hasta alcanzar el tamaño máximo especificado. Cuando se alcanza el límite, se crea un segundo archivo, utilizando el mismo nombre, al que se añade el dígito 2 al final del nombre. (Este es el punto en el que CAS empieza a intentar conectarse a un servidor secundario). Si dicho archivo también alcanza el tamaño máximo, se sobrescribe el primer archivo y, si el primer archivo se llena de nuevo, se sobrescribe el segundo archivo. Por lo tanto, después de una interrupción de larga duración, es posible que se pierdan datos, pero tendrá una cantidad de datos hasta el doble del límite del tamaño del archivo de sustitución por anomalía. El valor predeterminado es fail_over_file.	

Límite de tamaño del archivo de sustitución por anomalía	Tamaño máximo del archivo de sustitución por anomalía, en KB (el valor predeterminado es 5000). Hay dos de estos archivos, por lo que el requisito de espacio de disco será dos veces lo que especifique aquí. Si especifica -1, no habrá límite en el tamaño del archivo, pero se recomienda no hacerlo para limitar el tamaño del archivo.
Número máximo de intentos de reconexión	Después de perder una conexión con el sistema Guardium, el número máximo de veces que CAS intentará volver a conectarse. Establezca este valor en -1 para eliminar cualquier máximo (CAS intentará volver a conectarse de forma indefinida). El valor predeterminado es 5000 veces, de modo que, si se utiliza el intervalo de reconexión predeterminado, equivale aproximadamente a 3,5 días. Una vez alcanzado este máximo, CAS seguirá ejecutándose, escribiendo en los archivos de sustitución por anomalía, tal como se ha descrito anteriormente, pero no intentará volver a conectarse a un host.
Intervalo de reconexión	Número de segundos entre intentos de reconexión (60). Consulte la descripción del proceso de reconexión en **Número máximo de intentos de reconexión**.
Límite de datos en bruto	Número máximo de kilobytes escritos para un elemento cuando el recuadro de selección Conservar datos está marcado en la plantilla de un elemento (1000). Si especifica -1, no habrá límite.
Límite de tamaño de Md5	Tamaño máximo de un elemento de datos, por encima del cual no se realiza el cálculo de la suma de comprobación de MD5 (1000). Si especifica -1, no habrá límite.

Control de S-TAP - Identificación del usuario del servidor de aplicaciones

El producto de supervisión de ID de aplicación de usuario final utiliza el panel Identificación de usuario de servidor de aplicaciones. Póngase en contacto con el equipo de ventas o de soporte de Guardium si desea obtener más información sobre el producto de supervisión de ID de aplicación de usuario final.

Control	**Descripción**
Tiempo de espera de sesión	Número de minutos correspondiente un tiempo de espera excedido. El valor predeterminado es 1800.
Puertos	Puertos del servidor de aplicaciones. Utilice comas para separar las entradas, o guiones para rangos inclusivos. El valor predeterminado es 8080.
Patrón de inicio de sesión	Patrón utilizado para identificar un inicio de sesión de usuario.
Prefijo de nombre de usuario	Principio del nombre de usuario en los datos de Post/Get.
Postfijo de nombre de usuario	Fin del nombre de usuario en los datos de Post/Get.
Patrón de sesión	Patrón utilizado para identificar una sesión **nueva**.
Prefijo de sesión	Principio del ID de sesión en los datos de Post/Get.
Postfijo de sesión	Fin del ID de sesión en los datos de Post/Get.
Patrón de ID de sesión	Patrón utilizado para identificar una sesión **existente**.
Prefijo de ID de sesión	Principio del ID de sesión en los datos de Post/Get.
Postfijo de ID de sesión	Fin del ID de sesión en los datos de Post/Get.

Control de S-TAP - Hosts de Guardium

Este panel muestra todos los sistemas Guardium definidos como hosts para el S-TAP. En muchos casos, sólo habrá un sistema Guardium definido como el host para un S-TAP. Se pueden definir hosts adicionales para ofrecer funciones de sustitución por anomalía y de equilibrio de carga. Se hace referencia a los hosts del S-TAP de Guardium con estos tres términos:

Término	**Host de Guardium**
Host activo	El host al que está conectado actualmente este S-TAP. Si desea modificar la configuración del S-TAP, debe iniciar una sesión en el host activo. Normalmente, el host activo será el host primario.
Ho	El sistema Guardium elegido para recibir datos de este S-TAP y para controlar dichos datos. Este es el host al que el S-TAP intenta conectarse cada vez que se

st primario	reinicia S-TAP o después de restablecer la conexión con el host primario.
Host secundario	Si hay varios sistemas Guardium definidos como hosts para el S-TAP, cualquier sistema Guardium que no esté designado como host primario es un host secundario. Si el S-TAP pierde su conexión con el host activo y no puede volver a conectarse al host primario, intentará conectarse a un host secundario, en el orden listado. Cuando haya iniciado la sesión en la consola de administrador de un host secundario, podrá ver la configuración de S-TAP, pero no podrá editarla a menos que dicho host también sea el host activo en ese momento.

En el panel Configuración de S-TAP, el panel Host de Guardium contiene los controles que se describen aquí. Tenga en cuenta que los botones mostrados sólo están disponibles en el panel Configuración de S-TAP (no en el Panel de control de S-TAP):

Control	Descripción
Activo	Una marca de selección en esta columna indica el host activo para este S-TAP.
Host de Guardium	Identifica un sistema Guardium mediante la dirección IP o el nombre de host simbólico.
Suprimir	Pulse aquí para suprimir el host asociado. Este control no aparece en la fila del host activo.
Abajo	Pulse aquí para bajar el host una posición en la lista.
Arriba	Pulse aquí para subir el host una fila en la lista.
Marcar	Establecer como primario. Mover este host al principio de la lista y designarlo como host primario.

Control de S-TAP - Definir host de Guardium secundario

Antes de definir un host secundario, asegúrese de comprender cómo se utilizan los hosts. Consulte Hosts de Guardium secundarios para agentes de S-TAP en la visión general de Guía de administración de S-TAP.

Para definir un host secundario:

1. Pulse Gestionar > Supervisión de actividad > Control de A-TAP para abrir Control de S-TAP.
2. El primer host de la lista es el host primario para el S-TAP. Después de cualquier interrupción o reinicio, S-TAP intenta conectarse en primer lugar al host primario.
3. Especifique la dirección IP del host Guardium secundario en el recuadro de texto.
4. Pulse Añadir.
5. Opcional. Para cambiar el host designado como host primario (el primero de la lista) o para cambiar el orden de los hosts secundarios, realice una de las acciones siguientes:
   - Pulse Abajo o Arriba para reordenar la lista.
   - Pulse Establecer primario en la línea correspondiente a un host para moverlo al principio de la lista.
6. Opcional. Para eliminar un host secundario, pulse su botón Suprimir. No puede eliminar el host activo.
7. Cuando haya terminado, pulse Aplicar.

Nota: Si ha cambiado el host primario y desea que el S-TAP empiece inmediatamente a utilizar el nuevo host primario, y se trata de un servidor Windows, deberá reiniciar el servicio GUARD_STAP. No es necesario reiniciar el servicio en los servidores UNIX.

Control de S-TAP - Motores de inspección

El diseño del panel Motores de inspección varía en función del sistema operativo del servidor, del protocolo de la base de datos y, para los sistemas UNIX, de si se está utilizando el mecanismo T-Tap o TEE.

Nota: No configure un motor de inspección de S-TAP de modo que supervise el tráfico de red que también se supervisa directamente mediante un sistema Guardium que aloja el S-TAP, o mediante otro S-TAP que notifica al mismo sistema Guardium. Si esto sucede, el sistema Guardium recibirá información duplicada, no podrá reconstruir sesiones y pasará por alto ese tráfico.
Nota: Pulse Modificar para editar un motor de inspección.

Control	Descripción
Protocolo	El tipo de servidor de base de datos que se está supervisando (Aster, Cassandra, CouchDB, DB2, DB2 Exit, exclude IE, FTP, GreenPlumDB, Hadoop, HIVE, HTTP, HUE, IBM ISERIES, IMPALA, Informix, iNFORMIX Exit, KERBEROS, Maria,DB, MongoDB, MS SQL, Mysql, Named Pipes, Netezza, Oracle, PostgreSQL, SAP Hana, Sybase, Teradata, WebHDFS or Windows File Share).
Rango de puertos	Rango de puertos supervisados para este servidor de base de datos. Normalmente hay un único puerto en el rango. Para un motor de inspección de Kerberos, este valor siempre debe mostrar 88-88. Si se utiliza un rango, no incluya puertos adicionales en el rango, ya que esto puede dar lugar a un consumo excesivo de recursos cuando el S-TAP intenta analizar tráfico no deseado.
Puerto real Puerto escucha de TEE	No se utiliza para Windows. En UNIX, se ha sustituido por el puerto real de BD de KTAP cuando se utiliza el mecanismo de supervisión de K-Tap. Obligatorio cuando se utiliza el mecanismo de supervisión TEE. El puerto de escucha es el puerto en el que S-TAP escucha y acepta el tráfico de base de datos local. El puerto real es el puerto al que S-TAP reenvía el tráfico.
Puerto real de BD de K-TAP	No se utiliza para Windows. En UNIX, solo se utiliza cuando se utiliza el mecanismo de supervisión de K-Tap. Identifica el puerto de base de datos que debe supervisar el mecanismo K-Tap.
IP/máscara de cliente	Una lista de direcciones IP de cliente y máscaras correspondientes para especificar los clientes que se deben supervisar. Si la dirección IP es la misma que la dirección IP para el servidor de base de datos y se utiliza la máscara **255.255.255.255**, sólo se supervisará el tráfico **local**. El valor de dirección/máscara **1.1.1.1/0.0.0.0** supervisará todos los clientes. Cuando edite la lista, para crear una entrada de IP/máscara de cliente adicional, pulse Añadir. Para suprimir la última entrada de IP/máscara de cliente, pulse Suprimir. Si se especifica un valor de IP/máscara de cliente, no se puede especificar también Excluir IP/Máscara de cliente.
Excluir	Una lista de direcciones IP de cliente y máscaras correspondientes para especificar los clientes que se deben excluir. Esta opción le permite configurar el

IP/máscara de cliente	S-TAP de modo que supervise todos los clientes, excepto un determinado cliente o subred (o un conunto de estos). Cuando edite la lista, para crear una entrada Excluir IP/máscara de cliente adicional, pulse Añadir. Para suprimir la última entrada de Excluir IP/máscara de cliente, pulse Suprimir. Si se especifica un valor de Excluir IP/máscara de cliente, no se puede especificar también IP/Máscara de cliente.
Conectar a IP	La dirección IP de S-TAP que se utilizará para conectar a la base de datos. Algunas bases de datos solo aceptan conexiones en la IP real de la máquina y no en la dirección predeterminada (127.0.0.1).
Dir de instalación de BD	Solo UNIX. DB2, Informix u Oracle: especifique el nombre completo de la vía de acceso al directorio de instalación de la base de datos, por ejemplo, /home/oracle10. Todos los demás tipos de base de datos: especifique `NULL`.
Nombre de proceso	Para un servidor Windows: Sólo para Oracle o MS SQL Server, cuando se utilizan conductos con nombre. Para Oracle, la lista normalmente tiene dos entradas: **oracle.exe,tnslsnr.exe**. Para MS SQL Server, la lista suele ser sólo una entrada: **sqlservr.exe**. Para un servidor UNIX: Para una base de datos DB2, Oracle o Informix, escriba el nombre y vía de acceso completos del ejecutable de la base de datos. Por ejemplo: • Oracle: /home/oracle10/prod/10.2.0/db_1/bin/oracle • Informix: /INFORMIXTMP/.inf.sqlexec Informix: /INFORMIXTMP/.inf.sqlexec Se aplica a todas las plataformas Informix excepto Linux. Para Informix con Linux, ejemplo: /home/informix11/bin/oninit • MYSQL: mysql • PostgreSQL: POSTGRES.EXE, PG_CTL.EXE • Teradata: GTWGATEWAY.EXE • Para los demás tipos de bases de datos, especifique `NULL`
Cifrado	Activar el tráfico cifrado ASO o SSL para Oracle (versiones 11 y 12) y Sybase en Solaris, HPUX y AIX. Nota: Para Oracle 12 SSL, se necesitan pasos y configuración adicionales db_version=12 para la instrumentación y establecimiento de IE mediante guardctl. También se necesita instrumentación para Oracle versión 11 SSL en plataformas AIX.
Conductos con nombre	Sólo para Windows. Especifica el nombre del conducto con nombre que utiliza MS SQL Server para el acceso local. Si se utiliza un conducto con nombre, pero no se especifica nada aquí, S-TAP intenta recuperar del registro el nombre del conducto con nombre.
Nombre de instancia	El nombre de la instancia de base de datos es obligatorio para: • MS SQL Server 2005 que utiliza cifrado, o MS SQL Server que utiliza autenticación Kerberos (el valor predeterminado es MSSQLSERVER) • Oracle que utiliza el cifrado de base de datos (no hay valor predeterminado)
Memoria compartida de DB2	Los tres campos siguientes solo se aplica cuando se selecciona DB2 como tipo de base de datos. Si se supervisan las conexiones de memoria compartida, se deben establecer los tres parámetros siguientes.
Ajuste	El valor predeterminado es 20
Posición del cliente	El valor predeterminado es 61440.
Tamaño	El valor predeterminado es 131072
Identificador	El identificador es un campo opcional que se puede utilizar para diferenciar los motores de inspección entre sí. Si no especifica un valor para este campo, Guardium llenará automáticamente el campo con un nombre exclusivo utilizando el tipo de base de datos y el número de secuencia de visualización de la GUI.
Añadir	Cuando añada un motor de inspección, asegúrese de pulsar Añadir en el panel Añadir motor de inspección antes de pulsar Aplicar en el panel Configuración.

Pasar por alto la respuesta en el nivel de inspección

Utilice esta función para pasar por alto todas las respuestas de base de datos en el nivel de S-TAP, sin enviar nada al sistema Guardium.

En determinados entornos, en los que solo interesan las transacciones del cliente, esta función ahorra tiempo de proceso y ancho de banda tanto para el sistema S-TAP como para el sistema Guardium.

Utilice esta función para facilitar la configuración que permite pasar por alto las respuestas no deseadas de la base de datos, sin cargar la red.

[TAP] section DB_IGNORE_RESPONSE

Se puede obtener una lista de los tipos de base de datos separados por comas o se puede especificar ALL para pasar por alto las respuestas de todos los tipos de bases de datos; consulte el siguiente ejemplo. El valor predeterminado es none.

Si se establece en none, significa que no se pasa por alto ninguna respuesta.

Si se establece en all, significa que se pasan por alto las respuestas procedentes de todas las BD.

DB_IGNORE_RESPONSE=MSSQL,SYBASE,DB2

DB_IGNORE_RESPONSE=all

DB_IGNORE_RESPONSE=none

DB_IGNORE_RESPONSE_BYPASS_BYTES, el valor predeterminado es 1000

DB_IGNORE_RESPONSE_BYPASS_TIMEOUT, el valor predeterminado es 5 segundos

Estos son los tipos válidos de base de datos: ALL, CIFS, FTP, DB2_EXIT, PGSQL, MSSQL_NP, MSSQL, MYSQL, TRD, SYBASE, INFORMIX, DB2, ORACLE, KERBEROS.

Para añadir inspección CIFS/FTP, utilice puertos fijos para CIFS o FTP. FTP siempre utiliza el puerto 21; CIFS utiliza el puerto 139 o el puerto 445.

Es fácil configurar los motores de inspección para el tráfico FTP. Para una inspección neta, simplemente seleccione el protocolo FTP, especifique el puerto 21 y especifique las IP/máscaras tal como lo haría normalmente. Para S_TAP, seleccione el protocolo FTP, especifique 21 para todos los puertos y especifique las IP/máscaras (Dir de instalación de BD, Nombre de proceso y Conducto con nombre no se necesitan).

FTP Sniffing es la capacidad de ejecutar sniff sobre el tráfico FTP entre un cliente y un servidor como si fuese tráfico de base de datos. Con FTP, cualquier máquina puede ser un cliente (UNIX o Windows), y también cualquier sistema puede ser un servidor, siempre que haya un usuario válido con el que iniciar la sesión. Tenga en cuenta que no hay FTP local. Sin embargo, se puede ejecutar sniff en FTP mediante una inspección de red o mediante el sistema sniffing de S-TAP de red. El tráfico FTP normalmente aparecerá en el puerto 21. En GDM_CONSTRUCT, el tráfico FTP aparecerá como "_FTP" seguido del mandato RAW FTP que se ha enviado (tenga en cuenta que el mandato RAW FTP es diferente del FTP real que se ha enviado).

CIFS Sniffing (o Windows File Share Sniffing) es la capacidad de ejecutar sniff sobre la compartición de archivos Windows entre un cliente y un servidor como si fuera tráfico de la base de datos. Cuando se comparten directorios y archivos en Windows, este sistema de compartición se basa en el lenguaje smb o Samba, sobre el que el sistema Guardium ejecuta sniff y convierte en un lenguaje CIFS. Utilice la función smbclient para ejecutar sniff del tráfico de Windows File Share, pero también de las conexiones UNIX con carpetas compartidas de Windows. Tenga en cuenta que no hay CIFS local. Sin embargo, se puede ejecutar sniff en CIFS mediante una inspección de red o mediante el sistema sniffing de S-TAP de Windows. Tenga también en cuenta que no existe tal cosa como servidor CIFS. Cualquier máquina Windows puede compartir archivos o acceder a archivos compartidos, de modo que cualquier máquina Windows puede ser un cliente o un servidor. El tráfico de CIFS generalmente aparecerá en el puerto 139 o en el puerto 445. En GDM_CONSTRUCT, el tráfico de CIFS aparecerá como "_CIFS" seguido del mandato CIFS que se envió.

Control de S-TAP - Volver a cargar la última configuración correcta

Después de cambiar una configuración de S-TAP, es posible que note que su indicador luminoso de estado en el panel de control de S-TAP se vuelve amarillo. Una luz amarilla significa que hay una discrepancia entre la configuración en el sistema Guardium y la configuración en el S-TAP. Una luz amarilla temporal es aceptable, ya que el S-TAP tarda un tiempo en recibir y aprobar la nueva configuración. Si la luz amarilla persiste, suele significar que el S-TAP no ha aceptado la nueva configuración y ha vuelto a la última configuración correcta conocida.

Cuando se produzca un error, puede revisar los errores abriendo Informes > Informes operativos de Guardium en tiempo real > Sucesos de S-TAP. En la mayoría de los casos, el registro de sucesos contendrá mensajes de error que indicarán qué ha fallado con la nueva configuración. Consulte el apartado sobre visualización del panel de sucesos de S-TAP para obtener una descripción de los mensajes de error.

Configuración de S-TAP A-Tap - parámetros necesarios para supervisar la memoria compartida de DB2 en Linux

Los parámetros de S-TAP y A-Tap específicos de DB2 solo se aplican cuando se cumplen todas las condiciones siguientes:

- El servidor de DB2 se está ejecutando bajo Linux.
- El mecanismo de supervisión de K-Tap está instalado.
- Los clientes se conectan a DB2 utilizando la memoria compartida.

Los parámetros de S-TAP específicos de DB2 se establecen en el panel de definición del motor de inspección.

Establezca el valor del parámetro Position de acuerdo con el tamaño de la memoria compartida que utiliza db2bp, tal como se indica a continuación:

- Position=61440 (si db2bp utiliza 131072)
- Position=671744 (si db2bp utiliza 327680)
- Position=1064960 (si db2bp utiliza 524288)

Si no sabe el tamaño de la memoria compartida que utiliza db2bp, puede utilizar el procedimiento siguiente para encontrarlo.

Cómo encontrar los desplazamientos de la memoria compartida de db2

En la tabla siguiente se resumen los parámetros necesarios utilizados para S-TAP y A-Tap cuando se configuran para supervisar la memoria compartida de DB2 en Linux.

Parámetro	Nombre de S-TAP	A-Nombre de TAP	Valor predeterminado	Comentarios
Tamaño de cabecera de paquete	db2_fixed_pack_adjustment	db2_header_offset	20	El valor predeterminado se ha probado para DB2 8.2 y posteriores en diversas plataformas de 64 bits. Es posible que otras versiones de DB2 y plataformas de 32 bits necesiten un desplazamiento distinto. Los valores típicos son 16 y 12.
Desplazamiento del área de E/S de cliente	db2_shmem_client_position	db2_c2soffset	61440	Este parámetro se deriva del parámetro DB2 ASLHEAPSZ.
Tamaño de segmento de memoria compartida de DB2	db2_shmem_size	db2_shmsize	131072	Este parámetro se determina empíricamente.

Desplazamiento del área de E/S del cliente de cálculo (db2_shmem_client_position)

1. Abra un nuevo shell bash como usuario de la instancia de DB2.
2. Ejecute el mandato ps -x para verificar que el procesador de mandatos de db2bp no se está ejecutando actualmente para este shell. No debería ver el mandato denominado db2bp en ejecución. Si lo ve, puede interrumpirlo o ejecutar un nuevo shell.
3. Ejecute el mandato siguiente:

```
db2 get database manager configuration | awk '/ASLHEAPSZ/{print $9 * 4096}'
```

La salida es el valor necesario para db2_shmem_client_position.

El parámetro ASLHEAPSZ se especifica en páginas de memoria de 4K en DB2. Determina el tamaño del almacenamiento dinámico de la capa de soporte de la aplicación. Tal como se muestra en el diagrama anterior, el área de E/S del cliente se inicia inmediatamente después del almacenamiento dinámico de la aplicación en el segmento de memoria compartida del agente/aplicación.

Nota: La teoría detrás de este cálculo se basa en el documento DB2 Administration Guide: Performance.

Búsqueda de tamaño de segmento de memoria compartida de DB2 (db2_shmem_size)

A-TAP y K-TAP se basan en el tamaño para la identificación de los segmentos de memoria compartida de la aplicación/agente. Luego se interviene en estos segmentos mediante paquetes C2S y S2C. Para obtener información sobre cómo encontrar este valor, consulte el tema sobre búsqueda del tamaño de segmento de memoria compartida de DB2 en S-TAP de UNIX.

Tema principal: S-TAPs y otros agentes

Edición de los parámetros de configuración de S-TAP

Hay varias formas de modificar la configuración de un S-TAP después de instalarlo.

A veces, un usuario no puede tomar una decisión durante el proceso de instalación de un S-TAP o puede tomar una decisión equivocada que no se detecta hasta después de que se haya completado el proceso de instalación. Por ejemplo, un usuario puede olvidarse de escribir la dirección IP o puede utilizar una equivocada al definir un IP de protección de SQL. Estos tipos de errores se pueden remediar editando el archivo de configuración de S-TAP o modificando las configuraciones de S-TAP.

Si ha instalado S-TAP mediante Guardium Installation Manager (GIM), puede actualizar algunos parámetros a través de la API o la interfaz gráfica de usuario de GIM. Si no puede utilizar ninguno de estos métodos para actualizar los parámetros, puede editar el archivo de configuración en el servidor de datos.

En las tablas siguientes se proporciona una descripción detallada de los parámetros de S-TAP. Se indican los parámetros que se pueden actualizar mediante la interfaz gráfica de usuario de Guardium y mediante GIM.

Si es necesario modificar el archivo de configuración desde el servidor de base de datos, siga el procedimiento descrito. El archivo contiene comentarios que explican muchos de los parámetros.

1. Inicie la sesión en el sistema del servidor de base de datos utilizando la cuenta root.
2. Abra el archivo de configuración en un editor de texto.
3. Edite el archivo según sea necesario.
4. Guarde el archivo.
5. Reinicie S-TAP y verifique que el cambio ha sido incorporado.

- Parámetros de S-TAP de Windows
  En las tablas siguientes se definen los parámetros que se utilizan para controlar el comportamiento de los S-TAP en Windows.
- Parámetros de S-TAP de UNIX
  En las tablas siguientes se definen los parámetros que se utilizan para controlar el comportamiento de los S-TAP en UNIX.

Tema principal: S-TAPs y otros agentes

Parámetros de S-TAP de Windows

En las tablas siguientes se definen los parámetros que se utilizan para controlar el comportamiento de los S-TAP en Windows.

En las tablas se proporciona esta información para cada parámetro:

Parámetro
: El nombre del parámetro

Versión
: Si el parámetro se ha incorporado en la versión 8.0 o posterior, la versión más antigua con la que se puede utilizar el parámetro.

GUI
: Sí, si el parámetro se puede modificar mediante la interfaz de usuario de Guardium, en blanco si no es así.

Valor predeterminado
: El valor predeterminado del parámetro.

Descripción
: El significado de los parámetros, incluidas descripciones de los posibles valores.

Nota: Si la descripción de un parámetro empieza por "Avanzado", solo debe modificar el valor si es un usuario experto o si ha consultado a IBM.

- Parámetros de SQLGuard
  Estos parámetros describen un sistema Guardium al que se puede conectar este S-TAP.
- Parámetros generales
  Estos parámetros definen las propiedades básicas del S-TAP que se ejecuta en un servidor Windows y el servidor en el que está instalado y que no entran en ninguna de las otras categorías.
- Parámetros del motor de inspección
  Estos parámetros afectan al comportamiento del motor de inspección que utiliza S-TAP para supervisar un repositorio de datos en un servidor Windows.
- Parámetros de cortafuegos
  Estos parámetros afectan al comportamiento de S-TAP con respecto al cortafuegos.
- Parámetros del servidor de aplicaciones
  Estos parámetros afectan al comportamiento del S-TAP cuando se instala en una máquina cliente en lugar de en el servidor de base de datos.
- Parámetros de depuración
  Estos parámetros afectan al comportamiento de la depuración de S-TAP.
- Parámetros de CAS (Configuration Auditing System)
  Estos parámetros afectan al comportamiento de CAS en este sistema.
- Parámetros del controlador
  Estos parámetros afectan al comportamiento de diversos controladores con los que interactúa el S-TAP.

Tema principal: Edición de los parámetros de configuración de S-TAP

Parámetros de SQLGuard

Estos parámetros describen un sistema Guardium al que se puede conectar este S-TAP.

Tabla 1. Parámetros de configuración de S-TAP: SQLGuard

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
sqlguard_ip		Sí	Sí	NULL	Dirección IP o nombre de host del sistema Guardium que actúa como host para el S-TAP. Puede definir varios hosts añadiendo [SQLGuard_ 1], [SQLGuard_ 2] y así, sucesivamente.
primary		Sí	Sí	1	Indica si el servidor es un servidor primario: Windows: 0=NO, 1=SÍ. UNIX: 1=Primario, 2=Secundario, 3=Terciario, etc.

Tema principal: Parámetros de S-TAP de Windows

Parámetros generales

Estos parámetros definen las propiedades básicas del S-TAP que se ejecuta en un servidor Windows y el servidor en el que está instalado y que no entran en ninguna de las otras categorías.

Estos parámetros se almacenan en la sección [VERSION] del archivo de propiedades de S-TAP.

Tabla 1. Parámetros de configuración de S-TAP de la sección [VERSION]

Parámetro	Versión	GUI	Valor predeterminado	Descripción
stap_client_build				Solo lectura. La versión de compilación del S-TAP instalado
protocol_version				Solo lectura. La versión del sistema Guardium

Estos parámetros se almacenan en la sección [TAP] del archivo de propiedades de S-TAP.

Tabla 2. Parámetros de configuración de S-TAP de la sección [TAP]

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
tap_type					Solo lectura. STAP para UNIX, WTAP para Windows
tap_version					Solo lectura. La versión de S-TAP instalada en el servidor
tap_ip					Dirección IP o nombre de host para el sistema servidor de base de datos en el que está instalado S-TAP.
all_can_control		Sí		0	0 = S-TAP sólo se puede controlar desde el sistema Guardium primario. 1=S-TAP se puede controlar desde cualquier sistema Guardium.
participate_in_load_balancing				0	Controles de equilibrio de carga para los sistemas Guardium: • 0: No hay equilibrio de carga. • 1: Equilibrio de carga. El tráfico se equilibra entre el servidor primario y los secundarios, definidos en la sección SQLGuard. • 2: Redundancia. El S-TAP totalmente duplicado envía todo el tráfico al servidor primario y a los servidores secundarios, definidos en la sección SQLGuard. • 3: Equilibrio de carga de hardware. Guardium utiliza un equilibrador de carga como, por ejemplo, F5 o Cisco. S-TAP envía el tráfico al equilibrador de carga, que lo reenvía a uno de los recopiladores de la agrupación. Utilice el parámetro primary en la sección SQLGUARD para especificar los servidores primario, secundario, etc. Si este parámetro tiene el valor 0 y tiene más de un tráfico de supervisión del sistema Guardium, los sistemas Guardium no primarios están disponibles para la sustitución por anomalía.
connection_timeout_sec				60	Número de segundos tras los cuales el S-TAP considerará que el servidor Guardium no está disponible. Puede tener cualquier valor entero.
use_tls		Sí	Sí	0	1 = utilizar SSL para cifrar el tráfico entre el agente y el sistema Guardium. 0 = no cifrar. Aviso - el tráfico entre el agente y el sistema Guardium está en texto simple. Guardium recomienda cifrar el tráfico de red entre el S-TAP y el recopilador siempre que sea posible; este valor sólo se debe inhabilitar en los casos en los que el rendimiento sea una prioridad mayor que la seguridad.
failover_tls		Sí	Sí	1	1 = Si no es posible una conexión ssl por cualquier motivo, la sustitución por anomalía se realiza a la conexión no segura. 0=utilizar sólo conexiones seguras.
number_of_processors				4	Solo lectura. Número de procesadores de la máquina
alternate_ips				NULL	Lista separada por comas de direcciones IP virtuales o alternativas que se utilizan para conectar con este servidor de base de datos. Sólo se utiliza cuando el servidor tiene varias tarjetas de red con varias IP o IP virtuales. S-TAP sólo supervisa el tráfico cuando la IP de destino coincide con la IP de host S-TAP definida para este S-TAP o con una de las IP alternativas que se muestran aquí, por lo que recomendamos que liste aquí todas las IP virtuales.

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
db2_tap_installed				0	Establézcalo en 1 para el tráfico de memoria compartida de DB2 de sniffing. Inicia el servicio TAP de DB2 cuando está establecido en 1.
db2_exit_driver_installed		Sí			Integración de DB2 con S-TAP: establezca este valor en 1 para habilitar la integración de la biblioteca de salida de DB2 1) Dejar que S-TAP capture todo el tráfico de DB2 directamente desde el motor de DB2 - Tenga en cuenta que esto solo se aplica a releases específicos de DB2, de 10.1 en adelante 2) Cuando se utiliza este método, no se da soporte a la funcionalidad de cortafuegos ni de Scrub/Redact. Además, los procedimientos almacenados no se capturarán. 3) Permitir que el usuario elija todo el tráfico de DB2, independientemente del protocolo de cifrado/red. 4) Esta solución simplifica la configuración de S-TAP para los clientes que vayan a desplegar esta versión de DB2 y les ofrece soporte de DB2 nativo.
db2_shmem_driver_installed		Sí			Este parámetro ha quedado obsoleto y se ha sustituido por db2_tap_installed. Tenga en cuenta que este parámetro siempre se establece en 0 después de la instalación.
db2_shmem_driver_level					En desuso
dc_collect_freq	9			24	Especifica la frecuencia de la recopilación en horas. El mínimo es 1, el máximo es 24. GuardiumDC es un servicio que recopila actualizaciones de las cuentas de usuario (SID y nombres de usuario) del controlador de dominio primario y luego marca los cambios en Guardium_S-TAP para actualizar la correlación entre SID interno/nombre de usuario de S-TAP. Si S-TAP no encuentra el SID resuelto en la correlación, intenta obtenerlo desde el controlador de dominio primario, en cuyo caso S-TAP registra un mensaje en el registro de depuración (nivel 7) `El nombre de cuenta *** se ha recuperado para SID ***`.
dc_collect_maxusers	9			200,000	Número máximo de usuarios que se pueden recopilar. El valor mínimo es 10,000.
db_ignore_response	9				Pasar por alto la respuesta en el nivel de inspección. Utilice esta función para pasar por alto todas las respuestas de base de datos en el nivel de S-TAP, sin enviar nada al sistema Guardium. En determinados entornos, en los que solo interesan las transacciones del cliente, esta función ahorra tiempo de proceso y ancho de banda tanto para el sistema S-TAP como para el sistema Guardium. Utilice esta función para facilitar la configuración que permite pasar por alto las respuestas no deseadas de la base de datos, sin cargar la red. Se puede obtener una lista de los tipos de base de datos DB_IGNORE_RESPONSE de la sección [TAP] separados por comas o se puede especificar ALL para pasar por alto las respuestas de todos los tipos de bases de datos, por ejemplo DB_IGNORE_RESPONSE=ALL o DB_IGNORE_RESPONSE=MSSQL,DB2. Tipos de BD soportadas: ALL, MSSQL_NP, MSSQL, MYSQL, TRD, PGRS, MSSYB, ORACLE, DB2, DB2_EXIT, INFORMIX, KERBEROS, FTP, CIFS.
domain_controller	9				El nombre del controlador específico del que se debe leer la correlación entre SID y nombres de usuario.
high_resolution_timer				0	0: enviar indicaciones de fecha y hora en milisegundos. 1: enviar indicaciones de fecha y hora en microsegundos, pero utilizar el temporizador del sistema de milisegundos (para reducir el impacto en el rendimiento del sistema - multiplique los milisegundos por 1000). 2: enviar indicaciones de fecha y hora en microsegundos, utilizar el temporizador de Windows de alta resolución (más preciso). Para los casos 1 y 2, el S-TAP indicará al sistema Guardium que se envían microsegundos, estableciendo el byte reservado de PacketData en 1.
buffer_file_size				50	Tamaño, en MB, del almacenamiento intermedio asignado a la cola de paquetes
buffer_file_name					La vía de acceso completa del archivo correlacionado de memoria si BUFFER_MMAP_FILE=1. El valor predeterminado es carpeta de trabajo de WSTAP/StapBuffer/STAP_buffer.dtx
buffer_mmap_file	9			0	1 = opción de archivo correlacionado de memoria. 0 = asignación de memoria virtual
software_tap_host					Solo Windows - Identifica el host del servidor de base de datos en el que está instalado S-TAP. Puede ser una dirección IP o un nombre que el DNSserver reconozca. No hay valor predeterminado. Un SOFTWARE_TAP_HOST configurado de forma no válida se sustituye automáticamente por una IP local válida.
tcp_alive_message	9			1	1 = enviar mensajes de actividad a g-machine cada 5 segundos, confiando en la conexión TCP existente. 0 = enviar mensajes de actividad por parte de TCP en respuesta a mensajes procedentes de g-machine. Nota: Este parámetro se utiliza en versiones anteriores de Guardium (por ejemplo, v9.x). Los recopiladores de Guardium ya no envía mensajes de actividad UDP. Este parámetro ha quedado obsoleto en Guardium v10.x.
stack_trace_file_mode					Similiar a las opciones de volcado (dump)
minimum_heartbeat_interval				180	Solo Windows - El número de segundos que debe esperar S-TAP un latido procedente del sistema Guardium activo antes de intentar conmutar al siguiente servidor de su lista de sistemas Guardium.
tracefiles_dir					El directorio en el que se almacenarán los archivos del rastreador de accesos. El valor predeterminado es INSTALLDIR.
buffer_file_creation_max				3	No utilizado
compression_level				0	Nivel de compresión, entre 1 y 9. 0 = sin compresión.

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
disable_shared_memory_if_turned_on				0	
file_sniffer_frequency				45	Sólo para Windows. Frecuencia, en segundos, de: • intentos de registro con un sistema Guardium si un intento anterior no se ha ejecutado correctamente • S-TAP comprueba si hay nuevos registros disponibles en Program Files\IBM\Windows S-TAP\Logs para subirlos al recopilador
maximum_packet_num				300,000	En desuso
min_bytes_to_compress				500	Avanzado. Tamaño mínimo del mensaje a comprimir.
network_namedpipes		Sí		0	Avanzado
not_send_to_sqlguard				0	Avanzado. No enviar nada al sistema Guardium.
recv_level				0	Avanzado.
remote_messages		Sí		1	1 = Enviar mensajes al sistema Guardium activo. 0 = No enviar mensajes
send_level				0	Avanzada. Se utiliza para la prioritización de hebras.
sniffed_udp_ports				88	En desuso.
synch_flag				1	Solo lectura. Indica si los parámetros están sincronizados con la interfaz de usuario.
tap_dbserver_names					
tap_hb_udp_port				8075	Sólo para Windows. El número de puerto UDP por el que se envían los datos y los latidos a S-TAP desde cualquier sistema Guardium que vaya a actuar como servidor para este S-TAP
tap_min_heartbeat_interval				180	Número de segundos tras los cuales se realiza una sustitución por anomalía del S-TAP. Consulte también connection_timeout_sec para ver la sustitución por anomalía de S-TAP al recopilador secundario.
tcp_buffer_size				60000	Avanzado. Número mínimo de bytes que se deben recopilar antes de enviar un mensaje al sistema Guardium
time_network				0	Avanzado. Se utiliza solo para depuración.
user_collector_level				0	Avanzado.
web_server_connections				1	Número máximo de conexiones de BD por aplicación .net
web_server_installed				0	En desuso. Antes se utilizaba para habilitar el tap IIS.
web_server_port				9000	Puerto para web-server
guardium_ca_path				NULL	Ubicación del certificado de la entidad emisora de certificados.
sqlguard_cert_cn				NULL	El nombre común que se debe esperar del certificado de Sqlguard.
guardium_crl_path				NULL	La vía de acceso al directorio o archivo de lista de revocación de certificados.
tap_failover_session_quiesce				240	El número de segundos después de la sustitución por anomalía en que las sesiones no utilizadas de la lista de sustitución por anomalía de los servidores activos anteriores se pueden eliminar del servidor activo actual
tap_failover_session_size				8192	tamaño en MB de la lista de sesiones. 0 = ninguna sesión de sustitución por anomalía se debe guardar
db_ignore_response_filter				0.0.0.0/0.0.0.0	DB_IGNORE_RESPONSE_FILTER, valor predeterminado 0.0.0.0/0.0.0.0
db_ignore_response_local=1					DB_IGNORE_RESPONSE_LOCAL=1 Nota: El tráfico TCP no se considera tráfico local para el parámetro db_ignore_response_local.
db_ignore_response_bypass_bytes				65535	DB_IGNORE_RESPONSE_BYPASS_BYTES, valor predeterminado 65535
db_ignore_response_resets_per_request				1	DB_IGNORE_RESPONSE_RESETS_PER_REQUEST, valor predeterminado 1
upload_feature				1	Controla la carga de todos los archivos desde Program Files\IBM\Windows S-TAP\Logs en el recopilador

Tema principal: Parámetros de S-TAP de Windows

Parámetros del motor de inspección

Estos parámetros afectan al comportamiento del motor de inspección que utiliza S-TAP para supervisar un repositorio de datos en un servidor Windows.

Estos parámetros se almacenan en la sección de base de datos del archivo de propiedades de S-TAP, con el nombre de un repositorio de datos. Puede haber varias secciones en un archivo de propiedades, cada una de las cuales describa un motor de inspección utilizado por este S-TAP.

Tabla 1. Parámetros de configuración de S-TAP para un motor de inspección en Windows

Parámetro	Versión	GUI	Valor predeterminado	Descripción

Parámetro	Versión	GUI	Valor predeterminado	Descripción
db_type		Sí		El tipo de repositorio de datos que se está supervisando
instance_name		Sí		El nombre de la instancia de la base de datos en este servidor.
port_range_start		Sí		Rango de puertos inicial específico de la base de datos
port_range_end		Sí		Rango de puertos final específico de la base de datos
named_pipe		Sí		Nombre del conducto
networks		Sí		Identifica los clientes que se van a supervisar, mediante una lista de direcciones en formato dirección IP/máscara: n.n.n.n/m.m.m.m. No hay valor predeterminado. Para seleccionar todos los clientes, omita la lista de direcciones. Para seleccionar solo el tráfico local, utilice 127.0.0.1/255.255.255.255 Si se especifica una dirección/máscara IP incorrecta, el S-TAP no se iniciará.
exclude_networks		Sí		Una lista de direcciones IP de cliente y máscaras correspondientes para especificar los clientes que se deben excluir. Esta opción le permite configurar el S-TAP de modo que supervise todos los clientes, excepto un determinado cliente o subred (o un conjunto de estos). Cuando edite la lista para crear una entrada adicional Excluir dirección IP/máscara de cliente, pulse el botón Añadir. Para suprimir la última entrada Excluir dirección IP/máscara de cliente, pulse el botón Suprimir.
db_install_dir		Sí	NULL	Sólo Unix. DB2, Informix u Oracle: especifique el nombre completo de la vía de acceso al directorio de instalación de la base de datos. Por ejemplo: /home/oracle10 Todos los demás tipos de base de datos: especifique NULL
tap_db_process_names		Sí		Ejecutables en ejecución de la base de datos que se deben supervisan

Estos parámetros adicionales se utilizan con las bases de datos IBM DB2:

Tabla 2. Parámetros adicionales de configuración de S-TAP para un motor de inspección de DB2

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
db2_client_offset	8	Sí		61440	El desplazamiento con respecto a la parte del cliente del área de memoria compartida. El desplazamiento del cliente se puede calcular tomando el valor del parámetro ASLHEAPSZ de DB2 y multiplicándolo por 4096 para obtener el desplazamiento adecuado. El valor predeterminado para este parámetro es 61440 decimal. Este parámetro se calcula tomando el valor de configuración de base de datos de DB2 de ASLHEAPSZ y multiplicándolo por 4096. Para obtener el valor de ASLHEAPSZ, ejecute el siguiente mandato de DB2: db2 get dbm cfg y busque el valor de ASLHEAPSZ. Este valor suele ser 15, que da como resultado el valor predeterminado 61440. Si no es 15, tome el valor y multiplíquelo por 4096 para obtener el desplazamiento de cliente adecuado.
db2_fix_pack_adjustment	8	Sí		80	El desplazamiento con respecto a la parte del servidor del área de memoria compartida. El desplazamiento hasta el principio del paquete de memoria compartida de DB2 depende de la versión de DB2, 32 en las versiones anteriores, 80 en la versión 8.2.1 y posteriores.
db2_log_size	8	Sí		25	El tamaño máximo de archivo, en megabytes, que la DLL funcional puede mantener en el almacenamiento intermedio antes de empezar a descartar entradas de registro.
db2_shmem_client_position		Sí			Se debe establecer para supervisar el tráfico de memoria compartida de DB2.
db2_shmem_size		Sí		131072	Se debe establecer para supervisar el tráfico de memoria compartida de DB2.

Tema principal: Parámetros de S-TAP de Windows

Parámetros de cortafuegos

Estos parámetros afectan al comportamiento de S-TAP con respecto al cortafuegos.

Tabla 1. Parámetros de configuración de S-TAP para cortafuegos

Parámetro	Versión	GUI	Valor predeterminado	Descripción
firewall_installed			0	Función de cortafuegos habilitada. 1=sí, 0=no.
firewall_timeout			10	Tiempo en segundos que se debe esperar un veredicto del sistema Guardium si se ha excedido el tiempo de espera. Consulte el valor firewall_fail_close para saber si se debe bloquear o permitir la conexión. El valor puede ser cualquier valor entero.
firewall_fail_close			0	Si no se devuelve un veredicto desde el sistema Guardium y se pasa firewall_timeout, si firewall_close = 0 se permitirá la conexión; si firewall_close=1, la conexión se bloqueará.
firewall_default_state			0	Lo que desencadena el inicio de la modalidad de cortafuegos 0 = un suceso desencadena una regla en la política instalada 1 = iniciar en modalidad de cortafuegos habilitada independientemente de un suceso desencadenante (0). Este distintivo fuerza la observación (o habilitación) del cortafuegos independientemente de cualquier regla, pero las acciones específicas (DROP, etc) sólo se producen si las desencadena una regla.
firewall_force_watch	9.0		NULL	Cuando la característica de cortafuegos está habilitada y firewall_default_state es 0, la sesión se observará automáticamente cuando su IP de cliente coincida con una lista de valores de IP/MASK. La propia lista está separada por comas, por ejemplo 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2

Parámetro	Versión	GUI	Valor predeterminado	Descripción
firewall_force_unwatch	9.0		NULL	Cuando la característica de cortafuegos está habilitada y firewall_default_state es 1, la sesión se desatenderá automáticamente cuando su IP de cliente coincida con una lista de valores de IP/MASK. La propia lista está separada por comas, por ejemplo 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2,

Tema principal: Parámetros de S-TAP de Windows

Parámetros del servidor de aplicaciones

Estos parámetros afectan al comportamiento del S-TAP cuando se instala en una máquina cliente en lugar de en el servidor de base de datos.

Nota: Todos estos parámetros están en desuso para su uso en servidores Windows y no se deben modificar. Se muestran aquí porque es posible que los vea en el archivo de configuración.

Tabla 1. Parámetros de configuración de S-TAP para servidores de aplicaciones

Parámetro	Versión	GUI	Valor predeterminado	Descripción
appserver_installed			0	En desuso (solo para Windows). 0 es el valor predeterminado, S-TAP actúa de forma normal. 1 = S-TAP se establece en 'modalidad de cliente', conmuta los paquetes S2C y C2S para reflejar que el S-TAP se está instalando en el cliente, no en el servidor de bd. Además, si tiene el valor 1, realiza una comprobación para ver si se han definido otros parámetros appserver_* y, si es así, examina los paquetes http del puerto suministrado para obtener información de sesión sobre el usuario final de la aplicación java que reside en el sistema cliente.
appserver_ports		Sí	8080	En desuso (solo para Windows). Lista separada por comas de los puertos en los que se accede a la aplicación java a través del navegador web. Si mi url a un determinado almacén es: http://woodpecker:8888/estore, 8888 sería el valor que se suministra para este parámetro.
appserver_login_pattern		Sí		En desuso (solo para Windows). Lista de series separadas por comas que especifica el patrón de inicio de sesión que se pasa a la aplicación. Es el patrón que se pasa la aplicación java que indica un inicio de sesión de un usuario.
appserver_username_prefix		Sí		En desuso (solo para Windows). Lista de series separadas por comas que especifica el prefijo del nombre de usuario para una sesión determinada. Es el patrón que utiliza la aplicación java para indicar el nombre de usuario de una determinada sesión.
appserver_username_postfix		Sí		En desuso (solo para Windows). Lista de series separadas por comas que especifica el postfijo del nombre de usuario para una sesión determinada. Es el patrón (o carácter) que utiliza la aplicación java para indicar el final del valor para la variable especificada que indica el nombre de usuario.
appserver_session_pattern		Sí		En desuso (solo para Windows). Lista de series separadas por comas que especifica el inicio de una sesión de usuario final utilizando una determinada sesión de base de datos.
appserver_session_prefix		Sí		En desuso (solo para Windows). Lista de series separadas por comas que especifica dónde comienza el ID de sesión
appserver_session_postfix		Sí		En desuso (solo para Windows). Lista de series separadas por comas que especifica dónde termina el ID de sesión.
appserver_usersess_pattern		Sí		En desuso (solo para Windows). Lista de series separadas por comas que especifica el identificador para marcar la sesión final con la que está continuando una conexión determinada.
appserver_usersess_prefix		Sí		En desuso (solo para Windows). Lista de series separadas por comas que especifica lo que identifica o precede a session_id en un paquete de indicador del usuario determinado.
appserver_usersess_postfix		Sí		En desuso (solo para Windows). Lista de series separadas por comas que especifica dónde termina el ID de sesión.

Tema principal: Parámetros de S-TAP de Windows

Parámetros de depuración

Estos parámetros afectan al comportamiento de la depuración de S-TAP.

Estos parámetros se almacenan en la sección [DEBUG_OPTIONS] del archivo de propiedades de S-TAP:

Tabla 1. Parámetros de configuración de S-TAP para la depuración

Parámetro	Versión	GUI	Valor predeterminado	Descripción
debug_buffer			1	1=registrar el contenido de los paquetes locales
debug_firewall			1	1=registrar sucesos de cortafuegos

Estos parámetros se almacenan en la sección [TAP] del archivo de propiedades de S-TAP:

Tabla 2. Más parámetros de configuración de S-TAP para la depuración

Parámetro	Versión	GUI	Valor predeterminado	Descripción
debug_file_name				Ubicación del archivo de depuración de S-TAP. La ubicación predeterminada es c:/guardium/stap.txt

Parámetro	Versión	GUI	Valor predeterminado	Descripción
debug_max_file_size			200	
debuglevel			0	Nivel de mensajes de depuración que almacenar. Déjelo en 0 a menos que le indique lo contrario el equipo de soporte de IBM. 0 Sólo información de errores críticos Dos registros de depuración de "arranque" guardados en bin\..\logs. Sintaxis del nombre de archivo: startup_hostname_timestamp.new y startup_hostname_timestamp.old. Los archivos de bin\..\logs se suben automáticamente si upload_feature está activado. 1 Todos los mensajes anteriores más información de errores críticos repetidos Dos registros de depuración "normales guardados en bin\StapBuffer. Sintaxis del nombre de archivo: stap_hostname_timestamp.new y stap_hostname_timestamp.old. Los archivos de bin\StapBuffer no se suben. 2 No utilizado 3 Todos los mensajes del nivel 1, más información breve sobre los paquetes enviados a un sistema Guardium 4 Todos los mensajes del nivel 3, más el registro de sniffing local 5 Todos los mensajes del nivel 4, más el registro de sniffing de red 6 Todos los mensajes del nivel 5, más el registro de recepción de latidos 7 Todos los mensajes del nivel 6, más información variada de depuración
dump_file_mode			0	Habilita la captura de archivos de volcado si S-TAP se bloquea. Cuando el parámetro es distinto de cero, se abre un nuevo archivo de volcado cada vez que S-TAP se inicia; está vacío si no se produce un bloqueo. • 0: no se generan volcados de bloqueos • 1: se genera un archivo de volcados de bloqueo que se escribe en el archivo stap.diag que se crea en el directorio de trabajo de S-TAP. S-TAP copia cualquier archivo stap.diag existente en un archivo de copia de seguridad antes de sobrescribir el archivo stap.diag. • 2 : se generan volcados de bloqueo con indicación de fecha y hora, que se escriben en el archivo stap-INDICACIÓN_FECHA_HORA.diag que se crea en el directorio de trabajo de S-TAP, donde INDICACIÓN_FECHA_HORA incluye una serie de fecha y hora que identifica cuándo se ha generado el volcado del bloqueo. Si tiene problemas con bloqueos, utilice esta opción para capturar todos los volcados y no tan solo el más reciente. La indicación de fecha y hora también ayudará en la depuración. Sin embargo, esta opción utiliza más espacio de disco.
stack_trace_file_mode				parecido a dump_file_mode
kernel_debug_level			0	
syslog_messages			1	1 = enviar mensajes a syslog (para UNIX) o a EventViewer (para Windows). S0=no enviar mensajes.
WER_DUMP_FOLDER	10.2.30.15	N	Ninguno	Si el parámetro no está establecido, se determina de la siguiente manera. Si la carpeta de instalación del STAP se ha instalado como root en cualquier lugar que no sea C:\Program Files (x86)\... la carpeta de volcado WER se establecerá en la vía de acceso completa que finaliza con ...\Windows S-TAP\Bin\..\Logs. Si la carpeta de instalación de STAP contiene el texto "(x86)", la carpeta de volcado se establecerá en C:\Guardium\Dumps y dicha vía la creará el proceso de STAP. Por ejemplo, si el S-TAP de Windows se instala en C:\PROGRAM FILES\IBM\WINDOWS S-TAP y utiliza los valores predeterminados para WER_DUMP_FOLDER, WER_DUMP_COUNT, el S-TAP de Windows utiliza los siguientes valores de registro, entonces el volcado de los bloqueos se generarán a través del recurso WER (Windows Error Reporting) cuando se produzca un posible bloqueo. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\LocalDumps\guardium_stapr.exe DumpCount REG_DWORD 0x1 DumpFolder REG_EXPAND_SZ C:\PROGRAM FILES\IBM\WINDOWS S-TAP\Bin\..\LOGS\ DumpType REG_DWORD 0x2
WER_DUMP_COUNT	10.2.30.15	N	1	El valor máximo es 5.

Tema principal: Parámetros de S-TAP de Windows

Parámetros de CAS (Configuration Auditing System)

Estos parámetros afectan al comportamiento de CAS en este sistema.

Tabla 1. Parámetros de configuración de S-TAP para CAS

Parámetro	Versión	GIM	GUI	Valor predeterminado	Descripción
cas_task_checkpoint			Sí	task_checkpoint	
cas_client_checkpoint			Sí	client_checkpoint	
cas_checkpoint_period			Sí	60	Intervalo de tiempo, en segundos, para la comprobación
cas_fail_over_file			Sí	fail_over_file	Nombre del archivo que contiene el almacenamiento intermedio de mensajes de salida
cas_fail_over_file_size_limit			Sí	50000	Tamaño del archivo de sustitución por anomalía
cas_max_reconnect_attempts			Sí	5000	Número de intentos de reconexión cuando se pierde la conexión
cas_reconnect_interval			Sí	60	Tiempo de espera en segundos entre intentos de reconexión
cas_raw_data_limit			Sí	1000	Límite, en kilobytes, del tamaño de los datos sin formato que se envían al sistema Guardium
cas_md5_size_limit			Sí	1000	Tamaño del archivo mayor, en kilobytes, sobre el que se calcula MD5SUM
cas_command_wait	8.0			300	Tiempo de espera, en segundos, antes de interrumpir un proceso de recopilación de datos de larga duración
cas_server_failover_delay	8.0			60	Tiempo de espera, en minutos, antes de intentar conectar con otro sistema Guardium
cas_server_port					Sólo para Windows.

Tema principal: Parámetros de S-TAP de Windows

Parámetros del controlador

Estos parámetros afectan al comportamiento de diversos controladores con los que interactúa el S-TAP.

Tabla 1. Parámetros de configuración de S-TAP para controladores

Parámetro	Versión	GUI	Valor predeterminado	Descripción
tcp_driver_installed	v10		1	Utilizar el controlador TCP; el valor predeterminado es 1.
nptrc_log_size			2	Avanzado
shstrc_log_size			4	Avanzado
ora_driver_installed			1	Establézcalo en 1 para el tráfico SSL y ASO de Oracle de sniffing
ora_driver_level		Sí	0	Avanzada. Se utiliza para la prioritización de hebras.
named_pipes_driver_installed			1	Establézcalo en 1 para sniffing de conductos con nombre locales
named_pipes_driver_level		Sí	0	Avanzada. Se utiliza para la prioritización de hebras.
shared_memory_driver_level		Sí	0	Avanzada. Se utiliza para la prioritización de hebras.
krb_mssql_driver_installed			2	Establézcalo en 1 para el tráfico SSL de MSSQL de sniffing y para certificados Kerberos. Establezca su valor en 2 si desea recopilar solo el tráfico descifrado de MSSQL, pero no los certificados Kerberos, para ahorrar tiempo mediante la recopilación de los nombres de usuario del dominio al iniciar el programa. Tenga en cuenta que este parámetro siempre se establece en 0 después de la instalación. A partir de la V10.1, este parámetro se utiliza para habilitar/inhabilitar la correlación. Si se establece en un valor distinto de cero, se utiliza la correlación. Si es cero, no se utiliza la correlación. El valor predeterminado es un valor distinto de cero. Nota: Este parámetro ha quedado en desuso en la v10.1.4.
correlation_timeout			5	El número de segundos que los sniffers WFP y NMP esperan a que se produzca la correlación antes de abandonar y reanudar el flujo de tráfico al dispositivo. El valor predeterminado es 5 segundos.

Tema principal: Parámetros de S-TAP de Windows

Parámetros de S-TAP de UNIX

En las tablas siguientes se definen los parámetros que se utilizan para controlar el comportamiento de los S-TAP en UNIX.

En las tablas se proporciona esta información para cada parámetro:

Parámetro
: El nombre del parámetro

Versión
: Si el parámetro se ha incorporado en la versión 8.0 o posterior, la versión más antigua con la que se puede utilizar el parámetro

GUI
: Sí, si el parámetro se puede modificar mediante la interfaz de usuario de Guardium, en blanco si no es así

GIM
: Sí, si el parámetro se puede modificar mediante Guardium Installation Manager, en blanco si no es así

Valor predeterminado
: El valor predeterminado del parámetro

Descripción
: El significado de los parámetros, incluidas descripciones de los posibles valores

Nota: Si la descripción de un parámetro empieza por "Avanzado", solo debe modificar el valor si es un usuario experto o si ha consultado a IBM.

- Parámetros de SQLGuard
  Estos parámetros describen un sistema Guardium al que se puede conectar este S-TAP de Linux.
- Parámetros generales
  Estos parámetros definen las propiedades básicas del S-TAP que se ejecuta en un servidor de bases de datos y el servidor en el que está instalado y que no entran en ninguna de las otras categorías.
- Parámetros de Hadoop
- Parámetros del motor de inspección
  Estos parámetros afectan al comportamiento del motor de inspección que utiliza S-TAP para supervisar un repositorio de datos en un servidor de bases de datos.
- Parámetros de cortafuegos
  Estos parámetros afectan al comportamiento de S-TAP con respecto al cortafuegos.
- Parámetros del servidor de aplicaciones
  Estos parámetros afectan al comportamiento de los S-TAP cuando un nombre de usuario de la aplicación debe vincularse con actividades de la base de datos.
- Parámetros de descubrimiento
  Los parámetros de descubrimiento definen el comportamiento de la característica de descubrimiento automático, para descubrir instancias de bases de datos y enviar los resultados al S-TAP activo actual.
- Parámetros de CAS (Configuration Auditing System)
  Estos parámetros afectan al comportamiento de CAS en este sistema.
- Parámetros de depuración
  Estos parámetros afectan al comportamiento de la depuración de S-TAP.
- Parámetros de K-TAP
  Estos parámetros afectan al comportamiento del K-TAP.

Tema principal: Edición de los parámetros de configuración de S-TAP

Parámetros de SQLGuard

Estos parámetros describen un sistema Guardium al que se puede conectar este S-TAP de Linux.

Tabla 1. Parámetros de configuración de S-TAP: SQLGuard

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
sqlguard_ip		Sí	Sí	NULL	Dirección IP o nombre de host del sistema Guardium que actúa como host para el S-TAP. Puede definir varios hosts añadiendo [SQLGuard_ 1], [SQLGuard_ 2] y así, sucesivamente.
primary		Sí	Sí	1	Indica si el servidor es un servidor primario: Windows: 0=NO, 1=SÍ. UNIX: 1=Primario, 2=Secundario, 3=Terciario, etc.
sqlguard_port		Sí	Sí	16016	Solo lectura. Puerto utilizado para S-TAP para conectarse al sistema Guardium.
connection_pool_size	8.0	Sí	Sí	0	El número de conexiones que se abrirán entre el S-TAP y el proceso de sniffer en un host Guardium. Si se aumenta el valor se dispone de un rendimiento adicional que puede ser necesario cuando se habilita el cifrado como, por ejemplo TLS. El número máximo de conexiones agrupadas es de 50. El total es la suma de (connection_pool_size x num_main_threads) para todas las secciones [SQLGuard_n] en guard_tap.ini. Los valores válidos son: • 0: inhabilitar agrupación • 1-10 (para cada host definido) Valor predeterminado = 0
num_main_threads		Sí		1	El número de hebras utilizadas entre el S-TAP y uno o varios hosts de Guardium. Valores válidos: 1-510 (total máximo de 510 para todos los hosts de Guardium definidos) Valor predeterminado = 1 Nota: El equilibrio de carga de empresa no da soporte a la utilización de varias hebras para una sola unidad gestionada. Cuando se utilice el equilibrio de carga de empresa, establezca este parámetro en 1.

Tema principal: Parámetros de S-TAP de UNIX

Parámetros generales

Estos parámetros definen las propiedades básicas del S-TAP que se ejecuta en un servidor de bases de datos y el servidor en el que está instalado y que no entran en ninguna de las otras categorías.

Estos parámetros se almacenan en la sección [VERSION] del archivo de propiedades de S-TAP.

Tabla 1. Parámetros de configuración de S-TAP de la sección [VERSION]

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
stap_client_build			Sí		La versión de compilación del S-TAP instalado
protocol_version					La versión del sistema Guardium

Estos parámetros se almacenan en la sección [TAP] del archivo de propiedades de S-TAP.

Tabla 2. Parámetros de configuración de S-TAP de la sección [TAP]

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
tap_type					S-TAP para UNIX, W-TAP para Windows
tap_version					La versión de S-TAP que está instalada en el servidor
tap_ip			Sí		Dirección IP o nombre de host para el sistema servidor de base de datos en el que está instalado S-TAP.
devices		Sí	Sí	none	Interfaces que hay que escuchar. Utilice ifconfig para buscar la interfaz correcta.
all_can_control		Sí	Sí	0	0 = S-TAP sólo se puede controlar desde el sistema Guardium primario. 1=S-TAP se puede controlar desde cualquier sistema Guardium.
participate_in_load_balancing		Sí	Sí	0	Controles de equilibrio de carga para los sistemas Guardium: • 0: No hay equilibrio de carga. • 1: Equilibrio de carga. El tráfico se equilibra entre el servidor primario y los secundarios, definidos en la sección SQLGuard. • 2: Redundancia. El S-TAP totalmente duplicado envía todo el tráfico al servidor primario y a los servidores secundarios, definidos en la sección SQLGuard. • 3: Equilibrio de carga de hardware. Guardium utiliza un equilibrador de carga como, por ejemplo, F5 o Cisco. S-TAP envía el tráfico al equilibrador de carga, que lo reenvía a uno de los recopiladores de la agrupación. • 4: Varias hebras de S-TAP y almacenamientos intermedios KTAP se utilizan para dividir el tráfico. Utilice el parámetro primary en la sección SQLGUARD para especificar los servidores primario, secundario, etc. Si este parámetro tiene el valor 0 y tiene más de un tráfico de supervisión del sistema Guardium, los sistemas Guardium no primarios están disponibles para la sustitución por anomalía. Nota: Guardium no da soporte a la sustitución por anomalía con un recopilador v10.x S-TAP y un recopilador v9.x.
connection_timeout_sec			Sí	10	Número de segundos tras los cuales el S-TAP considerará que el servidor Guardium no está disponible. Puede tener cualquier valor entero.
use_tls		Sí	Sí	0	1 = utilizar SSL para cifrar el tráfico entre el agente y el sistema Guardium. 0 = no cifrar. Aviso: El tráfico entre el agente y el sistema Guardium está en texto simple. Guardium recomienda cifrar el tráfico de red entre el S-TAP y el recopilador siempre que sea posible; este valor sólo se debe inhabilitar en los casos en los que el rendimiento sea una prioridad mayor que la seguridad. No se da soporte a la descifrado de paquetes de inicio de sesión cuando TLS está habilitado. Esto significa que DB_USER no se cumplimenta y que los inicios de sesión anómalos no se asocian con un acceso.
failover_tls		Sí	Sí	0	1 = Si no es posible una conexión ssl por cualquier motivo, la sustitución por anomalía se realiza a la conexión no segura. 0=utilizar sólo conexiones seguras.
wait_for_db_exec			Sí	-1	

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción

tap_run_as_root	8.2		Sí	TAPUSER	Permitir que S-TAP se ejecute como usuario normal. 0 = el tap se ejecutará como usuario 'guardium', 1 = el tap se ejecutará como 'root'
					
					En casos excepcionales, tendrá que ejecutar el S-TAP como Guardium (y no root). Esto puede ocasionar otros problemas y sólo se debe utilizar cuando sea necesario. La ejecución de S-TAP como usuario de Guardium puede hacer que una base de datos o un protocolo dejen de funcionar debido a los niveles de permiso. Verifique que la vía de acceso de la base de datos o el archivo exec otorga permiso de lectura al usuario de Guardium. En función del entorno, las limitaciones típicas son:
					• Es posible que wait_for_db_exec no funcione. Para un clúster, compruebe la vía de acceso de la base de datos o el archivo exec para ver el permiso de lectura del usuario Guardium.
					• Es posible que la base de datos en WPAR de AIX y zonas de Solaris no funcione; compruebe el permiso para acceder a la vía de acceso de instalación o al archivo exec
					• Para Oracle BEQ, reinicie S-TAP después de iniciar o reiniciar la base de datos.
					• Para la memoria compartida de Informix, reinicie S-TAP después de iniciar o reiniciar la base de datos.
					• Para la memoria compartida de DB2, si shmctl ha fallado debido a un problema de permisos, en la mayoría de los casos se debe modificar S-TAP para que se ejecute como root.
					  ◦ Si el segmento de memoria compartida tiene permiso de lectura por grupo, asegúrese de que la instancia de DB2 se ha añadido al grupo de usuarios (Guardium). En cada servidor sólo se puede dar soporte a un conjunto de configuraciones de DB2.
					  ◦ Si el segmento de memoria compartida sólo tiene permiso de lectura para el usuario de db2, S-TAP se debe ejecutar como root. (Abra una sesión de memoria compartida de DB2, ejecute el mandato ipcs -ma, compruebe MODE en la salida)

tap_buf_dir				NULL	Ubicación del archivo de almacenamiento intermedio de S-TAP. El valor predeterminado es NULL y se colocará en $inidir/buffers
tap_log_dir				NULL	Ubicación de los archivos de registro S-TAP: guard_stap.stdout.tx, guard_stap.stderr.txt, guard_stap.fam.txt. El valor predeterminado es NULL. De forma predeterminada, los archivos se escriben en /tmp.
number_of_processors				4	Solo lectura. Número de procesadores de la máquina.
alternate_ips		Sí	Sí	NULL	Lista separada por comas de direcciones IP virtuales o alternativas que se utilizan para conectar con este servidor de base de datos. Sólo se utiliza cuando el servidor tiene varias tarjetas de red con varias IP o IP virtuales. S-TAP sólo supervisa el tráfico cuando la IP de destino coincide con la IP de host S-TAP definida para este S-TAP o con una de las IP alternativas que se muestran aquí, por lo que recomendamos que liste aquí todas las IP virtuales.
tee_installed			Sí	0	1 = Se está utilizando Tee. 0 = No se está utilizando Tee.
tee_msg_buf_len			Sí	128	Tamaño del almacenamiento correspondiente a Tee in MB. Puede adoptar cualquier valor entero.
buffer_file_size			Sí	50	Avanzado. Tamaño, en MB, del almacenamiento intermedio asignado a la cola de paquetes. Si el tamaño del almacenamiento intermedio es demasiado grande, es posible que el S-TAP no se pueda iniciar. Se sabe que los archivos de más de 2560 MB causan este problema.
buffer_file_name					La vía de acceso completa del archivo correlacionado de memoria si BUFFER_MMAP_FILE=1. El valor predeterminado es carpeta de trabajo de WSTAP/StapBuffer/STAP_buffer.dtx
buffer_mmap_file	9			0	1 = opción de archivo correlacionado de memoria. 0 = asignación de memoria virtual
tracefiles_dir		Sí			El directorio en el que se almacenarán los archivos del rastreador de accesos. El valor predeterminado es INSTALLDIR.
compression_level		Sí	Sí	0	Avanzado. Nivel de compresión, entre 1 y 9. 0 = sin compresión.
min_bytes_to_compress			Sí	500	Avanzado. Tamaño mínimo del mensaje a comprimir.
msg_aggregate_timeout				100	Tiempo en milisegundos durante el cual K-TAP envía los paquetes acumulados en su almacenamiento intermedio a S-TAP. Puede ser cualquier valor entero.
msg_count_watermark				64	Número de paquetes en los que K-TAP envía los paquetes acumulados en su almacenamiento intermedio a S-TAP. Puede ser cualquier valor entero.

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
log_program_name				0	Para aumentar el rendimiento, puede considerar la posibilidad de inhabilitar la obtención del nombre del programa de origen; al hacerlo, no podrá saber qué nombre de programa estaba utilizando la conexión (pero el resto de la información de conexión, como usuario y dirección de cliente, estarán disponibles). 0 = no enviar el nombre de source_program al sistema Guardium, 1 = enviar nombre de source_program al sistema Guardium.
max_server_write_size				16384	El número máximo de bytes que el S-TAP envía al sistema Guardium a la vez. Puede ser cualquier valor entero.
guardium_ca_path				NULL	Ubicación del certificado de la entidad emisora de certificados.
sqlguard_cert_cn				NULL	El nombre común que se debe esperar del certificado de Sqlguard.
guardium_crl_path				NULL	La vía de acceso al directorio o archivo de lista de revocación de certificados.
tap_failover_session_size				1024	El número máximo de sesiones de sustitución por anomalía de la lista por sistema Guardium. 0 = la característica de sustitución por anomalía está inhabilitada. Puede ser cualquier valor entero.
tap_failover_session_quiesce				240	El tiempo máximo de inactividad en minutos para la limpieza de listas de sesiones después de una sustitución por anomalía. El tiempo que debe transcurrir para que S-TAP considera que una sesión está 'muerta' (será el tiempo de limpieza para sesiones si transcurren failover_session_quiesce minutos después de una sustitución por anomalía) y cumple objetivos que incluyen: - está cerrada y no participa en una situación de sustitución por anomalía - S-TAP ha limpiado la política de la sesión y se ha eliminado de las listas de cortafuegos y de barrido.
kerberos_plugin_dir				NULL	Ubicación de los archivos de Kerberos.
db_ignore_response				NULL	Lista separada por comas de tipos de base de datos que se deben responder o pasar por alto. Si se establece en none, no se pasa por alto ninguna respuesta; si se establece en all, se pasan por alto las respuestas procedentes de todas las BD. Nota: Si se utiliza db_ignore_response=all para establecer que se pase por alto la respuesta de la base de datos de Oracle (no se captura para reducir la carga de tráfico), tenga en cuenta que hay más respuestas implicadas además de las del servidor de base de datos. Las respuestas del servidor de base de datos también pueden contener información importante de metadatos de protocolo de base de datos que utiliza la aplicación para la interpretación de las siguientes solicitudes de la base de datos.
stap_statistic				0	Intervalo en el que S-TAP envía información de estadísticas acerca de S-TAP/K-TAP a sniffer; 0 = no enviar. Especifique un entero positivo correspondiente a las horas o un entero negativo para los minutos.
stap_statistic_version				1	Las estadísticas de STAP son específicas de la versión del recopilador. 1: Guardium V10 y superior 0 - Guardium V9
upload_feature	9.1		Sí	1	Si = 1, cuando se cree un K-TAP nuevo, cárguelo automáticamente en el sistema Guardium al que informa este S-TAP. Puede definir este parámetro estableciendo el parámetro STAP_UPLOAD_FEATURE de GIM.
upload_snapshots				1	Subida automática de instantáneas
add_to_verification schedule				0	Añadir los motores de inspección definidos en guard_tap.ini a la planificación de la verificación de S-TAP. La verificación de STAP prueba la captura de tráfico. 0=DESACTIVADO, 1=ACTIVADO, el valor predeterminado es 0.
db_ignore_response_bypass_bytes			Sí	4096	Entero del tamaño de bytes del conjunto de resultados; cuando un conjunto de resultados es mayor que el tamaño se pasa por alto la respuesta.
db_ignore_response_resets_per_request			Sí	0	DB_IGNORE_RESPONSE_RESETS_PER_REQUEST, valor predeterminado 1
db_ignore_response_filter				0.0.0.0/0.0.0.0	Lista separada por comas de máscaras/direcciones IP cuyas respuestas serán ignoradas, de forma predeterminada filtra todo el tráfico Todas las respuestas de base de datos del tipo especificado en DB_IGNORE_RESPONSE para las máscaras/direcciones IP especificadas serán ignoradas. 0=no se filtran las respuestas 0.0.0.0/0.0.0.0=se filtran todas las direcciones IP
db_ignore_response_local				1	Filtro DB_IGNORE_RESPONSE_LOCAL de respuestas de bases de datos locales 0=no 1=sí

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
debug_snapshot				0	Para permitir que el registro de S-TAP obtenga información de depuración mediante la GUI (una vez establecido este valor mediante la GUI, los cambios no aparecerán en el archivo guard_tap.ini; pero, cuando se reinicia el proceso de S-TAP, estos valores del archivo ini se reflejarán en la GUI, lo que significa que se volverán a activar los valores predeterminados en la GUI).
debug_snapshot_level		Sí		1	Para establecer el nivel de depuración mediante la GUI: 0: Solo información de errores críticos; 1: Errores críticos más información de errores no críticos repetidos. 2: Comprobar si hay discrepancia de KTAP; se realizará una copia de seguridad de PCAP y se comprobarán los mensajes de STAP de GIM; más nivel 1. 3: Comprobar si el archivo de configuración guard_stap es válido más nivel 1. 4: Comprobar registro de sniffing local más nivel 1. 5: Comprobar registro de sniffing de red más nivel 1. 6: Comprobar información de depuración de Appserver más nivel 1. 7: Desencadenante para ejecutar script de diagnósticos más nivel 1.
debug_snapshot_time				60	Este parámetro se utiliza para definir el tiempo que se debe mantener la sesión iniciada de S-TAP a través de la GUI en segundos. El valor puede ser cualquier valor entero.
force_log_limited				0	Distintivo para manejar valores de sentencias SQL en S-TAP. 0 = sin restricciones. Valor predeterminado 1 = registros restringidos, enmascarar valores en sentencias SQL
hunter_trace			Sí	0	Habilitar UID_CHAIN 0: Inhabilitar. 1: Habilitar. Para conexiones TCP/IP locales, incluidas zonas de Solaris y WPAR de AIX; una conexión TCP/IP remota según appserver_installed = 1
load_balancer_ip		Sí	YES		Dirección IP de la unidad de equilibrio de carga.
load_balancer_num_mus				1	Número de unidades gestionadas para solicitar del equilibrador de carga
merge_with_template				0	Especifica si se tiene que fusionar la configuración desde el recopilador con el archivo de configuración de plantilla cuando la configuración se envía al STAP. 0=no 1=sí
shmid_blacklist				NULL	KATP utiliza shmid_blacklist para filtrar las conexiones de memoria compartida de los procesos que están separados con comas
shmid_blacklist_wait				0	Esperar para activar la interceptación hasta que se descubran elementos de shmid_blacklist 0: no, 1: sí (0)
blacklist_shmem_ops_by_proc				NULL	ktap utiliza blacklist_shmem_ops_by_proc para filtrar la interceptación de memoria compartida para los procesos especificados (lista separada por comas)
add_to_verification_schedule				0	
uid_chain_ssh_ip				0	Codificar la dirección IP del cliente en la cadena de UID cuando se identifica a sshd como uno de los procesos en la cadena. 0=inhabilitado, 1=habilitado

Tema principal: Parámetros de S-TAP de UNIX

Parámetros de Hadoop

Parámetros de guard_tap.ini para Hortonworks con Apache Ranger

Guardium da soporte a la integración de distribuciones Hortonworks mediante Apache Ranger. En la tabla siguiente se describen los parámetros de S-TAP necesarios para la conexión entre los S-TAP y los agentes Ranger.
Nota: Algunos parámetros se pueden configurar mediante la interfaz de usuario de Guardium o mediante Guardium Installation Manager. Todos los parámetros se pueden configurar con la API de Guardium.

Tabla 1. Parámetros de guard_tap.ini para Hortonworks con integración de Apache Ranger

Parámetro	Valores	Descripción

Parámetro	Valores	Descripción
log4j_reader_enabled	`0` ó `1` `0` está inhabilitado (valor predeterminado). `1` está habilitado.	Habilitar la modalidad de escucha log4j para el tráfico de Ranger.
log4j_port	Entero. El valor predeterminado es `5555`.	El puerto en el que el Guardium S-TAP escuchará las auditorías de Ranger.
log4j_listen_address	Dirección IP `0.0.0.0` indica cualquier dirección IP del sistema (valor predeterminado). `localhost` indica la dirección de bucle de retorno del sistema.	Los plugins de Ranger se conectarán a esta dirección. Se recomienda el valor predeterminado `0.0.0.0`, ya que permite al S-TAP recibir tráfico desde cualquier host. Utilice `localhost` si configura el sistema para alta disponibilidad. Si opta por restringir el acceso a una dirección específica, asegúrese de que no está excluyendo el tráfico necesario para la supervisión.
log4j_num_connections	Entero El valor predeterminado es `20`.	El número de conexiones simultáneas que se esperan del servicio o servicios definidos para este S-TAP.
ranger_dynamic_policy_reader_enabled	0, 1	Característica habilitada o no. 0=no, 1=sí
ranger_dynamic_policy_port	entero Valor predeterminado = 5556	Puerto al que se conectan los plugins de Ranger
ranger_dynamic_policy_listen_address	Valor predeterminado = 0.0.0.0	Dirección en la que escucha STAP Utilice localhost para HA
ranger_dynamic_policy_num_connections	Valor predeterminado = 20	Número de conexiones simultáneas
ranger_dynamic_policy_timeout	Valor predeterminado = 10	Número de segundos que se debe esperar un veredicto
ranger_dynamic_policy_default_verdict	0, 1 Valor predeterminado = 1	Comportamiento si el veredicto excede el tiempo de espera o si gmachine no está disponible 1 = coincide con política de Ranger 0 = no coincide con política de Ranger
ranger_dynamic_policy_reader_enabled	0 o 1 0 está inhabilitado (de forma predeterminada). 1 está habilitado.	Habilita la creación de registros de políticas dinámicas de Hortonworks.
ranger_dynamic_policy_port	Entero Valor predeterminado: 5556	Puerto en el que Guardium S-TAP está a la escucha de políticas dinámicas de Ranger.
ranger_dynamic_policy_listen_address	Dirección IP 0.0.0.0 indica cualquier dirección IP del sistema (valor predeterminado)	Plugins de políticas dinámicas de Ranger conectados a esta dirección.
ranger_dynamic_policy_num_connections	Entero El valor predeterminado es 20.	Número máximo de conexiones para el soporte desde el plugin de políticas dinámicas.
ranger_dynamic_policy_timeout	Entero El valor predeterminado es 10	Número de segundos que se debe esperar un veredicto antes de enviar el resultado del veredicto predeterminado.
ranger_dynamic_policy_default_verdict	0 o 1 1 = coincidencia, 0 = no coincidencia Valor predeterminado: 1	Comportamiento cuando no es posible acceder a Guardium o cuando se excede el tiempo de espera del veredicto.

Parámetros de guard_tap.ini para Cloudera Navigator que utiliza mensajería Kafka

Guardium da soporte a Cloudera Navigator para recopilar datos de auditoría mediante el sistema de mensajería Kafka.
Nota: Algunos parámetros se pueden configurar mediante la interfaz de usuario de Guardium o mediante Guardium Installation Manager. Todos los parámetros se pueden configurar con la API de Guardium.

Tabla 2. Parámetros de guard_tap.ini para Cloudera Navigator que utiliza la integración de mensajería de Kafka

Parámetro	Valores	Descripción
kafka_reader_enabled	`0` ó `1` `0` está inhabilitado (valor predeterminado). `1` está habilitado.	Habilitar la integración de Cloudera Navigator mediante publicación y consumo de Kafka.

Parámetro	Valores	Descripción
kafka_bootstrap_servers	Una lista separada por comas de pares `nombre host:puerto`. Formato: `host:puerto,host:puerto` Ejemplo: `hostnameofbroker1:9092,hostnameofbroker2:9092`	La lista `nombre host:puerto` se utiliza para establecer la conexión inicial con el clúster Kafka. Una vez establecida la conexión inicial, se utilizan todos los servidores del clúster. Es posible que desee especificar más de un programa de arranque en caso de que uno deje de estar activo.
kafka_use_tls	`0` ó `1` `0` está inhabilitado (valor predeterminado). `1` está habilitado.	Indicar si el clúster de Kafka utiliza TLS.
kafka_topic_name	Serie El valor predeterminado es `NavigatorAuditEvents`.	El nombre de tema que utiliza Cloudera Navigator para publicar sus sucesos de auditoría en Kafka.
kafka_principal	Serie El valor predeterminado es `NULL`.	El nombre de principal de Kerberos para el S-TAP, que se utiliza cuando el clúster de Kafka necesita autenticación de Kerberos.
kafka_keytab	NULL	La vía de acceso al archivo de tabla de claves de Kerberos en el servidor S-TAP.

Tema principal: Parámetros de S-TAP de UNIX

Parámetros del motor de inspección

Estos parámetros afectan al comportamiento del motor de inspección que utiliza S-TAP para supervisar un repositorio de datos en un servidor de bases de datos.

Estos parámetros se almacenan en la sección de base de datos del archivo de propiedades de S-TAP, con el nombre de un repositorio de datos. Puede haber varias secciones en un archivo de propiedades, cada una de las cuales describa un motor de inspección utilizado por este S-TAP.

Tabla 1. Parámetros de configuración de S-TAP para un motor de inspección en UNIX

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
db_type		Sí			El tipo de repositorio de datos que se está supervisando
port_range_start		Sí			Rango de puertos inicial específico de la base de datos
port_range_end		Sí			Rango de puertos final específico de la base de datos
networks		Sí			Identifica los clientes que se van a supervisar, mediante una lista de direcciones en formato dirección IP/máscara: n.n.n.n/m.m.m.m. No hay valor predeterminado. Para seleccionar todos los clientes, omita la lista de direcciones. Para seleccionar solo el tráfico local, utilice 127.0.0.1/255.255.255.255 Si se especifica una dirección/máscara IP incorrecta, el S-TAP no se iniciará.
tee_listen_port		Sí		12344	No se utiliza en Windows. En UNIX, se ha sustituido por el puerto real de BD de KTAP cuando se utiliza el mecanismo de supervisión de K-Tap. Obligatorio cuando se utiliza el mecanismo de supervisión TEE. El puerto de escucha es el puerto en el que S-TAP escucha y acepta el tráfico de base de datos local. El puerto real es el puerto al que S-TAP reenvía el tráfico.
connect_to_ip		Sí		127.0.0.1	Dirección IP de S-TAP que se utilizará para conectar a la base de datos. Cuando Tee esté habilitado, este parámetro será la dirección IP de S-TAP que se utilizará para conectar a la base de datos. Algunas bases de datos aceptan una conexión local en 127.0.0.1, mientras que otras solo aceptan una conexión local en la IP 'real' de la máquina y no en el valor predeterminado (127.0.0.1). Cuando K-TAP está habilitado, este parámetro se utilizará para zonas de Solaris y WPAR de AIX y debe ser la dirección IP de la zona para capturar tráfico.
exclude_networks		Sí			Una lista de direcciones IP de cliente y máscaras correspondientes para especificar los clientes que se deben excluir. Esta opción le permite configurar el S-TAP de modo que supervise todos los clientes, excepto un determinado cliente o subred (o un conjunto de estos). Cuando edite la lista para crear una entrada adicional Excluir dirección IP/máscara de cliente, pulse el botón Añadir. Para suprimir la última entrada Excluir dirección IP/máscara de cliente, pulse el botón Suprimir.
real_db_port		Sí		4100	No se utiliza en Windows. En Unix, solo se utiliza cuando se utiliza el mecanismo de supervisión de K-Tap. Identifica el puerto de base de datos que debe supervisar el mecanismo K-Tap.
db_install_dir		Sí		NULL	Sólo Unix. DB2, Informix u Oracle: especifique el nombre completo de la vía de acceso al directorio de instalación de la base de datos. Por ejemplo: /home/oracle10 Todos los demás tipos de base de datos: especifique NULL

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
db_exec_file		Sí		NULL	Para un servidor Windows: Sólo para Oracle o MS SQL Server, cuando se utilizan conductos con nombre. Para Oracle, la lista normalmente tiene dos entradas: oracle.exe,tnslsnr.exe. Para MS SQL Server, la lista suele tener una sola entrada: sqlservr.exe.Para un servidor Unix: Para una base de datos DB2, Oracle o Informix, escriba el nombre de vía de acceso completo del ejecutable de la base de datos. Por ejemplo: Oracle: /home/oracle10/prod/10.2.0/db_1/bin/oracle Informix: /INFORMIXTMP/.inf.sqlexec Se aplica a todas las plataformas Informix excepto Linux. Para Informix con Linux, ejemplo: /home/informix11/bin/oninit MYSQL: "mysql" Para todos los demás tipos de bases de datos, especifique NULL.
db_version		Sí		9	Versión de la base de datos. Se utiliza para capturar tráfico ATAP.
encryption		Sí		0	Activar el tráfico cifrado ASO o SSL para Oracle (versiones 11 y 12) y Sybase en Solaris, HPUX y AIX. Para Oracle, especifique db_version en el archivo ini (p.ej. db_version=12) Para Oracle12 SSL, instrumente en todas las plataformas. Para Oracle11 SSL, instrumente en AIX. Para cualquier Oracle que requiera instrumentación, si utiliza encryption=1 en guard_tap.ini (que no recibe soporte en Linux), debe instrumentar antes de definir este parámetro.
load_balanced		Sí	Sí	1	1 = la base de datos participa en el equilibrio de carga. 0 = la base de datos no participa en el equilibrio de carga.
unix_domain_socket_marker		Sí		NULL	Se utiliza para establecer el marcador para los sockets de dominio de Oracle, Mysql y Postgres. Generalmente el valor predeterminado es correcto, pero cuando el conducto con nombre o el tráfico de socket de dominio UNIX no funciona, es necesario asegurarse de que este valor se ha establecido correctamente. Por ejemplo, para Oracle, unix_domain_socket_marker se debe establecer en la clave del IPC definido en tnsnames.ora. Si es NULL o no está establecido, el S-TAP utilizará los marcadores predeterminados definidos como: * MySQL - "mysql.sock" * Oracle - "/.oracle/" * Postgres - ".s.PGSQL.5432"
instance_running				1	Para zonas de Solaris y WPAR, es posible que algunas zonas estén inactivas cuando se inicia S-TAP. En lugar de detener todo el S-TAP, si el distintivo wait_for_db_exec es distinto de cero, comprobaremos periódicamente si dicha zona se puede poner en funcionamiento. Si se puede, pasaremos el parámetro relevante al K-TAP y enviaremos una nueva configuración al sistema Guardium. La configuración mostrará qué bases de datos están activas o inactivas. Si instance_running es 1, lo que significa que la zona está activa, de lo contrario la zona está inactiva, el S-TAP comprobará si la instancia está activa periódicamente.
intercept_types		Sí		NULL	Inhabilita/habilita los tipos de interceptación para cada motor de inspección (IE), especificados como una lista de tipos separados por comas. Nulo: interceptación automática de todos los protocolos a los que la base de datos da soporte.
tap_identifier		Sí		NULL	Serie significativa para identificar la base de datos

Nota: Para el protocolo IPC de Informix en Solaris, el identificador de TAP no se asociará con el tráfico de la base de datos.

Estos parámetros adicionales se utilizan con las bases de datos IBM DB2:

Tabla 2. Parámetros adicionales de configuración de S-TAP para un motor de inspección de DB2

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
db2_fix_pack_adjustment	8	Sí		20	El desplazamiento con respecto a la parte del servidor del área de memoria compartida. El desplazamiento hasta el principio del paquete de memoria compartida de DB2 depende de la versión de DB2, 32 en las versiones anteriores, 80 en la versión 8.2.1 y posteriores.
db2_client_offset	8	Sí		61440	El desplazamiento con respecto a la parte del cliente del área de memoria compartida. El desplazamiento del cliente se puede calcular tomando el valor del parámetro ASLHEAPSZ de DB2 y multiplicándolo por 4096 para obtener el desplazamiento adecuado. El valor predeterminado para este parámetro es 61440 decimal. Este parámetro se calcula tomando el valor de configuración de base de datos de DB2 de ASLHEAPSZ y multiplicándolo por 4096. Para obtener el valor de ASLHEAPSZ, ejecute el siguiente mandato de DB2: db2 get dbm cfg y busque el valor de ASLHEAPSZ. Este valor suele ser 15, que da como resultado el valor predeterminado 61440. Si no es 15, tome el valor y multiplíquelo por 4096 para obtener el desplazamiento de cliente adecuado.
db2bp_path		Sí		NULL	En zonas de Solaris y WPAR de AIX, con la vía de acceso del ejecutable db2bp se podrá activar uid_chain para más de una instancia de db2 en un momento dado. El valor de este parámetro debe ser la vía de acceso completa del db2bp relevante tal como se ve desde la zona global/wpar. Por ejemplo, si el archivo es /data/db2inst1/sqllib/bin/db2bp y la zona está instalada en /data/zones/oracle2nd/root/, la vía de acceso completa a db2bp que se debe definir en el parámetro db2bp_path es /data/zones/oracle2nd/root/data/db2inst1/sqllib/bin/db2bp

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
db2_shmem_size				131072	Tamaño de segmento de memoria compartida de DB2

Tema principal: Parámetros de S-TAP de UNIX

Parámetros de cortafuegos

Estos parámetros afectan al comportamiento de S-TAP con respecto al cortafuegos.

Tabla 1. Parámetros de configuración de S-TAP para cortafuegos

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
firewall_installed			Sí	0	Función de cortafuegos habilitada. 1=sí, 0=no.
firewall_timeout			Sí	10	Tiempo en segundos que se debe esperar un veredicto del sistema Guardium si se ha excedido el tiempo de espera. Consulte el valor firewall_fail_close para saber si se debe bloquear o permitir la conexión. El valor puede ser cualquier valor entero.
firewall_fail_close			Sí	0	Si no se devuelve un veredicto desde el sistema Guardium y se pasa firewall_timeout, si firewall_close = 0 se permitirá la conexión; si firewall_close=1, la conexión se bloqueará.
firewall_default_state			Sí	0	Lo que desencadena el inicio de la modalidad de cortafuegos 0 = un suceso desencadena una regla en la política instalada 1 = iniciar en modalidad de cortafuegos habilitada independientemente de un suceso desencadenante (0). Este distintivo fuerza la observación (o habilitación) del cortafuegos independientemente de cualquier regla, pero las acciones específicas (DROP, etc) sólo se producen si las desencadena una regla. Nota: Si S-TAP está establecido para firewall_default_state= 1, el estado predeterminado para Consultar reescritura, grw_default_state= 1 no se puede establecer al mismo tiempo.
firewall_force_watch	9.0		Sí	NULL	Cuando la característica de cortafuegos está habilitada y firewall_default_state es 0, la sesión se observará automáticamente cuando su IP de cliente coincida con una lista de valores de IP/MASK. La propia lista está separada por comas, por ejemplo 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2
firewall_force_unwatch	9.0		Sí	NULL	Cuando la característica de cortafuegos está habilitada y firewall_default_state es 1, la sesión se desatenderá automáticamente cuando su IP de cliente coincida con una lista de valores de IP/MASK. La propia lista está separada por comas, por ejemplo 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2,

Tema principal: Parámetros de S-TAP de UNIX

Parámetros del servidor de aplicaciones

Estos parámetros afectan al comportamiento de los S-TAP cuando un nombre de usuario de la aplicación debe vincularse con actividades de la base de datos.

Tabla 1. Parámetros de configuración de S-TAP para servidores de aplicaciones

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
appserver_installed		Sí	Sí	0	0=S-TAP actúa de forma normal. 1 = S-TAP se establece en 'modalidad de cliente', conmuta los paquetes S2C y C2S para reflejar que el S-TAP se está instalando en el cliente, no en el servidor de bases de datos. Además, si tiene el valor 1, realiza una comprobación para ver si se han definido otros parámetros appserver_* y, si es así, examina los paquetes http del puerto suministrado para obtener información de sesión sobre el usuario final de la aplicación java que reside en el sistema cliente.
appserver_ports		Sí	Sí	8080	Lista separada por comas de los puertos en los que se accede a la aplicación Java a través del navegador web.
appserver_login_pattern		Sí	Sí		Lista de series separadas por comas que especifica el patrón de inicio de sesión que se pasa a la aplicación. Es el patrón que se pasa la aplicación Java que indica un inicio de sesión de un usuario.
appserver_username_prefix		Sí	Sí		Lista de series separadas por comas que especifica el prefijo del nombre de usuario para una sesión determinada. Es el patrón que utiliza la aplicación Java para indicar el nombre de usuario de una determinada sesión.
appserver_username_postfix		Sí	Sí		Lista de series separadas por comas que especifica el postfijo del nombre de usuario para una sesión determinada. Es el patrón (o carácter) que utiliza la aplicación Java para indicar el final del valor para la variable especificada que indica el nombre de usuario.
appserver_session_pattern		Sí	Sí		Lista de series separadas por comas especifica el inicio de una sesión de usuario final, utilizando una determinada sesión de base de datos. Este es el patrón que especifica [cambio de] sesión de usuario final para una conexión de base de datos determinada.
appserver_session_prefix		Sí	Sí		Lista de series separadas por comas que especifica el identificador de sesión
appserver_session_postfix		Sí	Sí		Lista de series separadas por comas que especifica dónde termina el ID de sesión.
appserver_usersess_pattern		Sí	Sí		Lista de series separadas por comas que especifica el identificador para marcar la sesión final con la que está continuando una conexión determinada.

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
appserver_usersess_prefix		Sí	Sí		Lista de series separadas por comas que especifica lo que identifica o precede a session_id en un paquete de indicador del usuario determinado.
appserver_usersess_postfix		Sí	Sí		Lista de series separadas por comas que especifica dónde termina el ID de sesión.

Tema principal: Parámetros de S-TAP de UNIX

Parámetros de descubrimiento

Los parámetros de descubrimiento definen el comportamiento de la característica de descubrimiento automático, para descubrir instancias de bases de datos y enviar los resultados al S-TAP activo actual.

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
discovery_interval				24	El intervalo de tiempo, en horas, que se ejecuta el descubrimiento automático. Establezca el valor 0 para inhabilitarlo.
discovery_dbs				oracle:db2:informix:mysql:postgres:sybase:hadoop:teradata:netezza:memsql	Lista de tipos de bases de datos a descubrir separados por caracteres de dos puntos(':').
discovery_debug				0	Nivel de depuración de descubrimiento 0 = solo errores 1 = errores y sentencias de depuración
discovery_ora_alt_locations					Ubicaciones alternativas en las que buscar archivos de listener.ora
discovery_port				8443	Puerto de Guardium que el descubrimiento de S-TAP utiliza para conectarse al sistema Guardium.

Tema principal: Parámetros de S-TAP de UNIX

Parámetros de CAS (Configuration Auditing System)

Estos parámetros afectan al comportamiento de CAS en este sistema.

Tabla 1. Parámetros de configuración de S-TAP para CAS

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
cas_task_checkpoint		Sí		task_checkpoint	
cas_client_baseline				client_baseline	
cas_client_checkpoint		Sí		client_checkpoint	
cas_checkpoint_period		Sí		3600	Intervalo de tiempo, en segundos, para la comprobación
cas_fail_over_file		Sí		fail_over_file	Nombre del archivo que contiene el almacenamiento intermedio de mensajes de salida
cas_fail_over_file_size_limit		Sí		50000	Tamaño del archivo de sustitución por anomalía
cas_max_reconnect_attempts		Sí		5000	Número de intentos de reconexión cuando se pierde la conexión
cas_reconnect_interval		Sí		60	Tiempo de espera en segundos entre intentos de reconexión
cas_raw_data_limit		Sí		1000	Límite, en kilobytes, del tamaño de los datos sin formato que se envían al sistema Guardium
cas_md5_size_limit		Sí		1000	Tamaño del archivo mayor, en kilobytes, sobre el que se calcula MD5SUM
cas_command_wait	8.0			300	Tiempo de espera, en segundos, antes de interrumpir un proceso de recopilación de datos de larga duración
cas_server_failover_delay	8.0			60	Tiempo de espera, en minutos, antes de intentar conectar con otro sistema Guardium

Tema principal: Parámetros de S-TAP de UNIX

Parámetros de depuración

Estos parámetros afectan al comportamiento de la depuración de S-TAP.

Estos parámetros se almacenan en la sección [DEBUG_OPTIONS] del archivo de propiedades de S-TAP:

Tabla 1. Parámetros de configuración de S-TAP para la depuración

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
debug_buffer				1	1=registrar el contenido de los paquetes locales

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
debug_firewall				1	1=registrar sucesos de cortafuegos

Estos parámetros se almacenan en la sección [TAP] del archivo de propiedades de S-TAP:

Tabla 2. Más parámetros de configuración de S-TAP para la depuración

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
syslog_messages				1	1= envía mensajes a syslog. 0 = no enviar mensajes.
tap_debug_output_level					Nivel de registro de STAP. Los registros son guard_stap.stderr.txt, guard_stap.stdout.txt, guard_stap.fam.txt que se encuentran en el directorio especificado en el parámetro tap_log_dir. Niveles de registro de STAP: • 0: Solo información de errores críticos • 1: Información de errores críticos más información de errores no críticos repetidos • 2: Comprobar si KTAP está inactivo, entonces se volverá a activar PCAP más nivel 1 • 3: Comprobar si el archivo de configuración guard_stap es válido más nivel 1 • 4: Comprobar registro de sniffing local más nivel 1 • 5: Comprobar registro de sniffing de red más nivel 1 • 6: Comprobar información de depuración de Appserver más nivel 1 • 7: Desencadenante para ejecutar script de diagnósticos más nivel 1
remote_messages		Sí		1	• 0 = No enviar mensajes • 1 = Enviar mensajes al host SQL Guard activo.

Tema principal: Parámetros de S-TAP de UNIX

Parámetros de K-TAP

Estos parámetros afectan al comportamiento del K-TAP.

Tabla 1. Parámetros de configuración de K-TAP

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
ktap_installed			Sí	1	¿Está instalado el módulo del supervisor de kernel?: 0=NO, 1=SÍ. ktap_installed y tee_installed son mutuamente excluyentes; sólo se puede activar uno.
ktap_request_timeout	8.0			5	Es el tiempo de espera excedido de espera de una respuesta de K-TAP. K-TAP envía ioctl a stap para solicitar información y espera la respuesta de stap. Se expresa en segundos y puede tener cualquier valor.
ktap_dbgev_ev_list	8.0			0	Se utiliza para habilitar el registro de rastreo de K-TAP mediante la GUI o mediante el archivo guard_tap.ini: 0=inhabilitar, 1=habilitar el registro de rastreo de ktap ubicado en el directorio /var/tmp
ktap_dbgev_func_name	8.0			all	Lista de funciones que se deben registrar en el registro de rastreo de K-TAP. all=todas las funciones, o bien se puede especificar una función específica como, por ejemplo accept, para registrar en el archivo de registro únicamente las funciones de aceptación. Si especifica una función que no es relevante para el registro de rastreo de K-TAP, no se registrará nada en el registro.
ktap_fast_tcp_verdict	8.0			1	Para una conexión tcp, K-TAP enviará ioctl a stap para confirmar que la sesión es la conexión de base de datos configurada en nuestro IE, mediante la comprobación de Ips. Si ktap_fast_tcp_verdict tiene el valor 1, K-TAP no enviará la solicitud a S-TAP siempre y cuando los puertos de la sesión estén dentro del rango. Puede adoptar el valor 1 ó 0 (0)
ktap_fast_file_verdict	8.0			1	Para una conexión tli, K-TAP enviará ioctl a S-TAP para confirmar que dicha sesión es la conexión de base de datos configurada en el IE, mediante la comprobación de los puertos e Ips; si ktap_fast_file_verdict tiene el valor 1, K-TAP no enviará la solicitud a S-TAP, siempre y cuando los puertos de la sesión estén dentro del rango. Puede adoptar el valor 1 ó 0 (1).
ktap_buffer_size	8.0			4194304	Avanzado. Tamaño del almacenamiento intermedio de K-TAP en bytes. El rango de valores es el comprendido entre 1 MB y 16 MB
ktap_buffer_flush	8.0			0	Avanzado. La forma de enviar mensajes de K-TAP a S-TAP. Si = 1, el S-TAP lee todo el almacenamiento intermedio de K-TAP y procesa todos los paquetes del almacenamiento intermedio. Si ktap_flush_buffer=0, el S-TAP lee una cantidad fija en lugar de todo el almacenamiento intermedio.
ktap_local_tcp	8.2			0	1=interceptar únicamente las conexiones locales (aunque se seguirán capturando las conexiones interceptadas anteriormente) (este parámetro se utiliza para conexiones TCP)
khash_table_length	8.0			24593	Número de sesiones que se pueden almacenar en la tabla Khash. Es un entero y puede tener cualquier valor.
khash_max_entries	8.0			8192	Longitud de la tabla que contiene toda la información correspondiente a la sesión específica. Es un entero y puede tener cualquier valor.

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
ktap_fast_shmem	9			1	Para la conexión de memoria compartida de db2 • 0=KTAP envía ioctl al STAP para confirmar que la sesión es la conexión de base de datos configurada en el motor de inspección (IE) comprobando el ID de proceso. • 1= K-TAP no envía la solicitud al S-TAP siempre que el db2_shmem_size de la sesión coincida con el segmento de memoria adjunto.
fam_enable				1	Habilitación/inhabilitación global de FAM
ktap_fsmon_buffer_size				4194304	Tamaño del almacenamiento intermedio de FAM

Tabla 2. Parámetros de configuración de A-TAP y PCAP

Parámetro	Versión	GUI	GIM	Valor predeterminado	Descripción
atap_exec_location				/var/guard	Ubicación del ejecutable que se utiliza cuando se activa ATAP habilitando el recuadro de cifrado en la sección del motor de inspección
pcap_read_timeout	8.0			0	Sólo tráfico pcap (no ktap): el tiempo que debe esperar STAP entre el muestreo de pcap. Este valor sólo se debe modificar si así lo indican los servicios de Guardium, después de examinar el problema y de determinar las pérdidas (no se captura todo el tráfico) debidas a un cuello de botella relacionado con pcap/stap.
pcap_dispatch_count	8.0			16	Optimización de la captura de pcap; el número de paquetes que empaquetar (agrupar) antes de informar a stap. Al agrupar agrupando paquetes se reduce la comunicación de pcap a stap, lo que mejora el rendimiento. Este valor sólo se debe modificar si así lo indican los servicios de Guardium, después de examinar el problema y de determinar las pérdidas (no se captura todo el tráfico) debidas a un cuello de botella relacionado con pcap/stap.
pcap_buffer_size	8.0			-1	Tamaño del almacenamiento intermedio del socket pcap. Este parámetro solo se utiliza en LINUX. El valor predeterminado de este entero es -1, lo que significa obtener el máximo almacenamiento intermedio posible. En cualquier otro caso, este tamaño de almacenamiento intermedio está en kilobytes. 0 no es válido - si es cero 0, significa 60; si no es este, puede ser cualquier valor hasta un máximo de 65535. Un almacenamiento intermedio mayor significa que probablemente habrá menos pérdidas cuando haya ráfagas de alto volumen de tráfico. Escenario: ráfagas de mucho tráfico, pcap lo captura todo, pero el stap (el flujo de pcap a stap) no es lo suficientemente rápido y no puede gestionar el tráfico. Para evitar pérdidas, los paquetes pendientes de proceso se colocan en el almacenamiento intermedio. Cuanto mayor es el almacenamiento intermedio, más posibilidad hay de poder gestionar ráfagas altas y prolongadas de mucho tráfico. Este valor sólo se debe modificar si así lo indican los servicios de Guardium, después de examinar el problema y de determinar las pérdidas (no se captura todo el tráfico) debidas a un cuello de botella relacionado con pcap/stap.
	8.0			1	Cuando este parámetro está habilitado, siempre inicia PCAP independientemente de si ktap_installed está habilitado o si no lo está, en la medida que DB2 esté definido en el motor de inspección (IE).

Adición de parámetro para controlar el uso de la distribución de módulos KTAP a través de la GUI de GIM

Usuarios de GIM - Compile un KTAP incorporado personalizado en un lote personalizado y utilícelo en otros servidores de base de datos.

Usuarios que no sean de GIM - No se necesitan lotes personalizados; KTAP personalizado se puede compilar y copiar entre el servidor de base de datos de forma manual.

Nombre del parámetro: GIM_ALLOW_CUSTOM_BUNDLES

Valores válidos: '1' - permitir instalaciones de lotes personalizados. '0' - Rechazar instalaciones de lotes personalizados

Valor predeterminado: 1

Durante una instalación desde cero de GIM (servidor de BD) - El usuario puede especificar un nuevo parámetro de instalación opcional, --install_custom_bundles.

Si se especifica, se permitirán instalaciones de lotes personalizados (por ejemplo, lote personalizado STAP) (GIM_ALLOW_CUSTOMED_BUNDLES tendrá el valor '1') en dicho servidor de BD. De lo contrario, no se permitirán (GIM_ALLOW_CUSTOMED_BUNDLES tendrá el valor '0').

Durante una actualización de GIM (mediante la GUI de GIM) desde una versión de GIM que NO tenga este parámetro - El valor predeterminado será '1' (para no inhabilitar esta funcionalidad para los clientes que puedan haber estado utilizando hasta ahora esta función).

Este parámetro puede tener el valor '1' ó '0' cuando se utiliza el programa de utilidad configurador en el servidor de BD.

Este parámetro no se puede establecer en '1' desde la GUI si el valor anterior es '0'.

Nota: Esta funcionalidad se comprobará durante la instalación (en el servidor de BD), NO mientras esté asignando o planificando una instalación de lotes o una actualización de parámetros (como se validan todos los demás parámetros).

Características afectadas: BUNDLE-GIM, configurator.sh, instalador consolidado

Mandatos GuardAPI y lote KTAP personalizado

En v10

1. El indicador STAP_UPLOAD_FEATURE está activado de forma predeterminada (1) para que los KTAP se suban al dispositivo cuando se compilen automáticamente

2. Para poder compilar un lote GIM personalizado para que incluya un nuevo KTAP personalizado, el usuario debe ejecutar el mandato make_bundle_with_uploaded_kernel_module de grdapi (es necesario especificar la sintaxis exacta del mandato)
3. Para poder utilizar el lote personalizado ya compilado en cualquier servidor, el cliente debe activar el indicador GIM_ALLOW_CUSTOM_BUNDLES en 1 (por razones de seguridad esto tiene que realizarse manualmente en cada servidor de BD). El indicador GIM_ALLOW_CUSTOM_BUNDLES se puede volver a desactivar desde el dispositivo.

Tema principal: Parámetros de S-TAP de UNIX

Configuración del montaje retardado en disco de clúster

Este tema sólo se aplica a los servidores de base de datos Oracle, Informix y DB2.

Para estos tipos de bases de datos, cuando se inicia el S-TAP, debe tener acceso al directorio de inicio de la base de datos. Si su entorno utiliza un esquema de clúster en el que varios nodos comparten un único disco que está montado en el nodo activo, pero no en el nodo pasivo, el directorio de inicio de la base de datos no está disponible en el nodo pasivo hasta que se produce la sustitución por anomalía.

Se puede configurar la carga retardada de S-TAP definiendo una propiedad del archivo de configuración, WAIT_FOR_DB_EXEC. Cuando se inicia, si S-TAP encuentra que no hay acceso al directorio de inicio de la base de datos, comprueba el valor de WAIT_FOR_DB_EXEC y realiza la acción adecuada.

- WAIT_FOR_DB_EXEC > 0, S-TAP se inicia independientemente de si puede stat() nombre proceso. Intenta stat () nombre proceso cada 15 minutos
- WAIT_FOR_DB_EXEC < = 0 S-TAP intenta stat() nombre proceso en el motor de inspección (IE) inmediatamente después de iniciarse. Si no puede stat() nombre proceso, S-TAP finaliza.

Antes de definir para esta propiedad un valor positivo, asegúrese de definir todas las demás propiedades de configuración necesarias y probar que S-TAP se inicia y recopila los datos correctamente. Esta propiedad solo se puede establecer editando el archivo de configuración y no desde la interfaz gráfica de usuario.

Tema principal: Configuración especial de entornos Linux, Solaris, HP-UX y AIX
Tema principal: S-TAPs y otros agentes

Supervisor de estado de S-TAP

El supervisor de estado de S-TAP le permite ver el estado actual de los S-TAP e investigar los problemas.

Vaya a Gestionar > Vista del sistema > Supervisor de estado de S-TAP, donde puede ver el estado de cada S-TAP.

Pulse en cualquier línea de la lista para ver los motores de inspección que están configurados para este S-TAP. Los rastros de navegación muestran dónde se encuentra; pulse Todos los S-TAP para volver a la lista de S-TAP.

La lista de motores de inspección muestra si se han verificado. Si un motor de inspección no está verificado, puede enviarlo para su verificación inmediatamente o puede añadirlo a la planificación de verificación existente. Se da soporte a la verificación para estos tipos de base de datos:

- DB2
- Greenplum
- Informix
- MSSQL
- MySQL
- Netezza
- Oracle
- PostgreSQL
- Sybase
- Teradata (solo verificación avanzada)

Si selecciona el recuadro que hay junto a una base de datos de un tipo no soportado, se visualiza un mensaje que indica que el tipo no recibe soporte para la verificación. Hay dos tipos de verificación:

Verificación estándar
: Comprueba el S-TAP y el motor de inspección enviando una solicitud de inicio de sesión no válida, para verificar que devuelve el mensaje de error adecuado.

Verificación avanzada
: Si necesita evitar solicitudes de inicio de sesión erróneo, puede utilizar la verificación avanzada. Para este tipo, debe identificar o crear una definición de origen de datos asociada con la base de datos de destino. La definición de origen de datos incluye credenciales, que el proceso de verificación utiliza para iniciar la sesión en la base de datos. Luego envía una solicitud para recuperar datos de una tabla no existente a fin de generar un mensaje de error.

Para ambos tipos de solicitudes de verificación, los resultados se muestran en un diálogo nuevo que proporciona información sobre las pruebas que se han realizado y las acciones recomendadas para las pruebas que han fallado.

De forma predeterminada, el sistema espera cinco segundos antes de mostrar los resultados de la verificación. Si la latencia de la red es alta, es posible que no sea suficiente para recibir la respuesta esperada de servidor de bases de datos. Si tiene que permitir más tiempo, puede utilizar el mandato de CLI store stap network_latency para cambiar el periodo.

Temas relacionados:

- Visualización de los resultados de la verificación de S-TAP
- Configuración de la planificación de verificación de S-TAP
- Resolución de problemas de S-TAP en la plataforma Linux

Tema principal: S-TAPs y otros agentes

Visualización de los resultados de la verificación de S-TAP

El proceso de verificación de S-TAP comprueba varios parámetros de configuración e intenta conectarse a los motores de inspección. Puede ver los resultados en la página Supervisor de estado de S-TAP.

Antes de conectarse a la base de datos, el proceso de verificación comprueba si el proceso sniffer se está ejecutando en el sistema Guardium. El proceso sniffer es responsable de comunicarse con cada S-TAP y de procesar los datos que se reciben. Si el sniffer no se está ejecutando, las respuestas de S-TAP no se reconocen.

El proceso de verificación intenta iniciar una sesión en la base de datos con un ID de usuario y una contraseña erróneos, para verificar que este intento se reconoce y se comunica al sistema Guardium. El S-TAP podría estar configurado de forma que evitara que el mensaje llegara al sistema Guardium desde el que se ha realizado la solicitud.

Estos detalles de configuración incluyen:

- Equilibrio de carga: si el S-TAP está configurado para devolver respuestas a más de un sistema Guardium, el mensaje de error se podría enviar a un sistema Guardium diferente.
- Sustitución por anomalía: Si se han configurado sistemas Guardium secundarios para el S-TAP, el mensaje de error podría enviarse a un sistema Guardium secundario si el sistema Guardium primario está demasiado ocupado.
- Db_ignore_response: si el S-TAP está configurado para pasar por alto todas las respuestas de la base de datos, no envía mensajes de error al sistema Guardium.
- IP/máscara de cliente: si se ha definido alguna máscara que no sea 0.0.0.0, podría impedir que se enviara el mensaje de error.
- Excluir IP/máscara: Si se ha definido alguna máscara que no sea 0.0.0.0, podría impedir que se enviara el mensaje de error.

A continuación, el proceso de verificación comprueba si se puede conectar con el motor de inspección de seleccionado en el servidor de base de datos. Espera recibir una respuesta que indique un inicio de sesión fallido. Si se recibe una respuesta diferente, es posible que tenga que seguir investigando.

Algunos mensajes de error de bases de datos individuales no indican un problema específico. Por ejemplo, en varias bases de datos soportadas, el código de error devuelto para un puerto incorrecto también puede significar que la propia base de datos no se ha iniciado.

Los resultados del proceso de verificación se visualizan en un diálogo. Primero se muestran las comprobaciones fallidas, con recomendaciones para los pasos siguientes. Las comprobaciones correctas se muestran en una sección contraída al final de la lista. En algunas situaciones, puede ser útil revisar las comprobaciones correctas para elegir entre los posibles pasos siguientes.

Temas relacionados:

- Supervisor de estado de S-TAP
- Resolución de problemas de S-TAP en la plataforma Linux
- Configuración de la planificación de verificación de S-TAP

Tema principal: S-TAPs y otros agentes

Configuración de la planificación de verificación de S-TAP

Puede configurar la planificación para ejecutar la verificación de S-TAP.

Acerca de esta tarea

De forma predeterminada, la planificación para verificar los S-TAP es una vez por hora, cada día. Se utiliza la misma planificación para todos los S-TAP cuya verificación está planificada. Puede cambiar esta planificación.

Procedimiento

1. Pulse Gestionar > Supervisión de actividad > Planificador de verificación de S-TAP para abrir el Planificador de verificación de S-TAP.
2. En la parte del Planificador de verificación de S-TAP de la página, pulse Modificar planificación.
3. En el diálogo Definición de planificación, utilice las listas desplegables y los recuadros de selección para planificar la ejecución de la verificación. Esta planificación se aplica a todos los S-TAP cuya verificación está planificada.
4. Pulse Guardar para guardar los cambios.

Tema principal: S-TAPs y otros agentes

Resolución de problemas de S-TAP en la plataforma Linux

Puede utilizar el separador del supervisor de estado de S-TAP de la vista del sistema para empezar a investigar cualquier problema. A veces, es posible que tenga que utilizar otras herramientas, especialmente si está supervisando bases de datos para las que no se pueden verificar los motores de inspección.

- Si un S-TAP no está conectado a su sistema Guardium, compruebe si el proceso de S-TAP se está ejecutando en el servidor de base de datos:

  UNIX: Verifique que el proceso de S-TAP se está ejecutando
  En el servidor de bases de datos, desde la línea de mandatos ejecute el mandato ps -ef | grep stap para verificar que el proceso de S-TAP se está ejecutando.
  En la lista de procesos, busque /guardium/guard_stap.

- **Linux**: Ejecute debug desde la línea de mandatos para identificar rápidamente problemas de configuración, con la sintaxis <programa_stap> <archivo_parámetros> <nivel_depuración>, donde 4 es el nivel correspondiente a la depuración norma. (Otros valores hacen cosas diferentes, no todos depuran). Por ejemplo: /usr/local/guardium/guard_stap/guard_stap /usr/local/guardium/guard_stap/guard_tap.ini 4
- Verifique la conexión entre el servidor de base de datos y el sistema Guardium.
  - Verifique que puede ejecutar ping en el sistema Guardium en *sqlguard_ip* desde el servidor de base de datos.
  - Si ping se ejecuta correctamente, verifique que puede establecer una conexión telnet con los siguientes puertos en el sistema Guardium: 16016/16018
- Si hay un cortafuegos entre el servidor de base de datos y el sistema Guardium, verifique que los puertos siguientes están abiertos para el tráfico entre estos dos sistemas: Puerto TCP 16016 o puerto TLS 16018 para conexiones cifradas.
  Nota: Utilice el siguiente mandato para comprobar la disponibilidad de los puertos: `nmap -p puerto nombrehost_o_ip_guardium`
- Verifique que el parámetro sqlguard_ip está establecido en el valor correcto de *nombrehost_o_ip_guardium* para el sistema Guardium con el que se va a conectar.
  1. Pulse Gestionar > Supervisión de actividad > Control de A-TAP para abrir Control de S-TAP.
  2. Localice el host S-TAP para la dirección IP que corresponda a su servidor de base de datos.
  3. Expanda la subsección Hosts Guardium y verifique que el host Guardium esté correctamente configurado.
  4. Si es necesario, pulse Modificar para actualizar los Hosts Guardium.
- Verifique que el proceso de S-TAP no se reinicia continuamente: En el servidor de base de datos, ejecute el mandato `ps -eaf | grep stap` para verificar que el proceso para S-TAP no está cambiando.

- Verifique que la aprobación de S-TAP no está activada. Si la aprobación de S-TAP está activada, se rechaza cualquier nuevo S-TAP que se conecte al sistema Guardium.
    1. Pulse Gestionar > Supervisión de actividad > Certificación de S-TAP para abrir Certificación de S-TAP.
    2. Busque el recuadro de selección Aprobación necesaria de S-TAP. Si este recuadro está seleccionado, los nuevos S-TAP solo se pueden conectar a este sistema Guardium después de que se hayan añadido a la lista de S-TAP aprobados.
    3. Si la aprobación de S-TAP está activada, seleccione Supervisor diario > Clientes Tap aprobados para ver una lista de los S-TAP aprobados. Si el S-TAP que está investigando no está en esta lista, vuelva al panel Certificación de S-TAP, especifique la dirección IP del S-TAP en el campo Host de cliente y pulse Añadir.

Si el S-TAP muestra el estado verde pero no se procesan datos, compruebe el estado del A-TAP.

Temas relacionados:

- Supervisor de estado de S-TAP
- Visualización de los resultados de la verificación de S-TAP
- Supervisión del comportamiento de S-TAP

Tema principal: S-TAPs y otros agentes

Supervisión del comportamiento de S-TAP

S-TAP Monitor (guard_monitor) es un proceso diseñado para supervisar el rendimiento y la capacidad de respuesta de S-TAP. Se pueden llevar a cabo determinadas acciones en función de diversos umbrales.

En el caso de UNIX/Linux, el rendimiento de la CPU se comprueba con el mandato *ps*. La capacidad de respuesta se comprueba enviando al proceso de S-TAP una solicitud de consola y esperando una respuesta.

Si la utilización de CPU de S-TAP supera el umbral configurado, o si S-TAP no responde a la solicitud de la consola, se pueden llevar a cabo las acciones siguientes:

- Ejecutar guard_diag automáticamente
- Interrumpir automáticamente el proceso S-TAP.
- Volcar el núcleo automáticamente e interrumpir el proceso S-TAP.

Nota: S-TAP Monitor está disponible en UNIX/Linux y Windows.

Tabla 1. Qué se supervisa, UNIX/Linux

UNIX/Linux
Uso de CPU
Memoria
Interrupción (Kill)
Volcado del núcleo
Ejecutar diagnósticos
"Actividad" - Reacción (sondeo de CPU)

guard_monitor no está habilitado de forma predeterminada.

En instalaciones de Shell, debe habilitarse desde inittab descomentando la línea "umon" o utilizando el recurso de control de servicios para los sistemas operativos concretos (initctl para RedHat 6 y siguientes, SMF para Solaris 10 y superiores).

Para instalaciones de GIM, guard_monitor se habilita estableciendo

STAP-UTILS_START_MONITOR=y

Nota: Guard_monitor requiere privilegios administrativos (root).

La ubicación predeterminada de la salida de S-TAP Monitor es /var/tmp/monitor. Esta ubicación se puede configurar desde guard_monitor.ini (archivo de configuración) - consulte el ejemplo del archivo guard_monitor.ini al final de este tema.

Después de habilitar guard_monitor, asegúrese de que el proceso está en ejecución en el servidor de base de datos.

Nota: guard_monitor se ejecuta con su archivo de configuración, guard_monitor.ini, como su argumento. El supervisor se controla utilizando el archivo guard_monitor.ini. Para instalaciones de shell, puede hacer todos los cambios de configuración directamente en el archivo de configuración. Para GIM, utilice la interfaz de la GUI para realizar los cambios.
Nota: Después de la instalación de S-TAP, Guard Monitor se instala automáticamente. No hay solicitudes de usuario ni se muestra ningún progreso de la instalación. Durante la desinstalación de S-TAP, Guard Monitor se desinstala automáticamente. El usuario ya no tiene la opción de rearrancar en el instalador y, en su lugar, simplemente se le notifica que es necesario un rearranque para completar la desinstalación. Este rearranque no es crítico, pero es necesario si el usuario tiene intención de volver a instalar S-TAP en el sistema. Si el usuario realiza la desinstalación, no reinicia y, a continuación, intenta reinstalar aparecerá un mensaje emergente bloqueando la instalación y notificando al usuario que S-TAP está parcialmente instalado y que es necesario rearrancar el servidor.

Ejemplos de valores

Se proporcionan umbrales predeterminados para cada función. Por ejemplo, es posible que desee supervisar el uso de CPU y establecer un umbral (75%) para la recopilación de información de diagnóstico y un umbral superior (85%), en el que se debe interrumpir S-TAP. Debería establecer auto_diag=1 para habilitar la recopilación de información de diagnósticos y diag_high_cpu_level=7500 para recopilar información cuando el uso de CPU alcance el 75%. A continuación, debería establecer auto_kill_on_cpu_enable=1 para habilitar la interrupción automática del proceso S-TAP y establecer auto_kill_on_cpu_level=8500 para interrumpir el proceso cuando la CPU alcance el 85%.

auto_kill_on_cpu_level=8500 para interrumpir el proceso cuando la CPU alcance el 85%.

Si no desea mantener la interrupción del proceso S-TAP repetidamente, aquí también puede establecer un límite. Puede limitar el número de veces que se puede interrumpir el proceso dentro de una hora estableciendo kill_num_in_hour=5. Y a continuación, puede especificar lo que debe ocurrir cuando se alcance el límite: codifique final_action= 1 para inhabilitar S-TAP o final_action= 2 para que pueda continuar su ejecución.

Parámetros de sondeo de CPU de guard_monitor

De forma predeterminada, guard_monitor comprueba la utilización de la CPU de STAP cada 10 segundos, tal como se define en:

poll_cpu_interval=10 (parámetro de guard_monitor.ini)

STAP-UTILS_MONITOR_POLL_CPU_INTERVAL =10 (Interfaz de GIM)

Guard_monitor también envía una solicitud de S-TAP de consola cada 10 segundos, tal como se define en:

poll_stap_interval=10

STAP-UTILS_MONITOR_POLL_STAP_INTERVAL =10

Cuando se comprueba la utilización de la CPU, guard_monitor mide la utilización media de la CPU durante la vida del proceso guard_stap mediante *ps*. Esto quiere decir que STAP tiene que ejecutarse por encima del umbral de CPU durante algún tiempo antes de que guard_monitor detecte un problema.

Solo en plataformas Linux, Guardium da soporte a una medición más precisa de la CPU de S-TAP, basada en la utilización media de CPU en un intervalo de tiempo:

cpu_measurement_timeslice=5

Acción de diagnóstico automático

Si la utilización de CPU de S-TAP excede el umbral configurado, la acción más básica que toma guard_monitor es un guard_diag automático.

Primero, habilite guard_diags automático:

auto_diag=1 (guard_monitor.ini)

STAP-UTILS_MONITOR_AUTO_DIAG =1 (GIM)

A continuación, defina el umbral de CPU de STAP en el que guard_monitor iniciará un guard_diag:

diag_high_cpu_level=7500 (parámetro de guard_monitor.ini)

STAP-UTILS_MONITOR_DIAG_HIGH_CPU_LEVEL=7500 (parámetro de GIM)

Nota: Los niveles de CPU se introducen en múltiplos de 100 para evitar problemas de coma decimal con la salida de *ps*.

El supervisor puede crear más de una salida de guard_diag, tal como se define en los parámetros:

diag_num=2 (guard_monitor.ini)

STAP-UTILS_MONITOR_DIAG_NUM=2 (GIM)

La salida de guard_diag se ubica en /var/tmp

Acción de interrupción automática

Además de generar la salida de guard_diag, el supervisor también puede interrumpir automáticamente el proceso S-TAP.

Habilite la interrupción automática de S-TAP:

auto_kill_on_cpu_enable=1 (guard_monitor.ini)

STAP-UTILS_MONITOR_AUTO_KILL_ON_CPU_ENABLE =1 (GIM)

Defina el umbral de CPU de STAP en el que guard_monitor interrumpirá S-TAP:

auto_kill_on_cpu_level=8500 (parámetro de guard_monitor.ini)

STAP-UTILS_MONITOR_AUTO_KILL_ON_CPU_LEVEL=8500 (parámetro de GIM)

Puede limitar el número de veces que guard_monitor se interrumpe en una hora:

kill_num_in_hour=5 (guard_monitor.ini)

STAP-UTILS_MONITOR_KILL_NUM_IN_HOUR =5 (GIM)

¿Qué sucede si se alcanza el número máximo de interrupciones por hora? Inhabilite S-TAP (1) o detenga la interrupción de S-TAP y deje que continúe (2) mediante la configuración de final_action:

final_action=2 (guard_monitor.ini)

STAP-UTILS_MONITOR_FINAL_ACTION =2 (GIM)

Volcado del núcleo de S-TAP antes de interrumpir

Algunos problemas de S-TAP, como cuando S-TAP se cuelga en un bucle, requieren más información de la que se proporciona en la salida de guard_diag.

Una novedad de Guardium v10.0 es el volcado automático del núcleo del proceso S-TAP por parte de guard_monitor. guard_monitor realiza un volcado automático del núcleo de S-TAP antes de interrumpir el proceso (si la interrupción automática de S-TAP está habilitada).

Hay dos parámetros para configurar los volcados de núcleo automáticos:

force_core_before_kill=< sigsegv| gcore|pstack>

kill_oldcore_saved=1

force_core_before_kill es un parámetro de serie de caracteres que especifica el tipo de volcado del núcleo que se debe generar:

sigsegv: Esta es la más portátil de las opciones, pero requiere que SA configure ulimit para habilitar la creación de volcados del núcleo.

gcore: La opción más útil, pero requiere que gcore esté instalado en el sistema.

pstack: La más simple de las opciones. Puede ser el único programa de utilidad disponible en determinados sistemas.

kill_old_core_saved es un parámetro entero. Cuando se establece en un valor distinto de cero, guard_diag conserva todos los volcados de núcleo generados. De lo contrario, suprime los volcados de núcleo antiguos cada vez que se genera uno nuevo.

Ubicación de volcados de núcleos creados por guard_monitor: /var/tmp/monitor/coredumps

Ejemplo de guard_monitor.ini

```
; La siguiente cabecera de sección se necesita para que GIM reconozca este archivo .ini.

; por lo demás, no tiene ningún objetivo concreto

[TAP]

; dir salida para registros, diagnósticos, rastreos, etc. del supervisor.

monitor_output_dir=/var/tmp

; ubicación de la instalación de guardium (no es necesario que sea donde está el supervisor, por ejemplo /usr/local)

stap_dir=/usr/local

; ip a la que conectar para descargar el archivo de configuración y subir la salida de diagnósticos y rastreo

; se analiza en guard_tap.ini, pero el valor de reserva se conserva sincronizado

sqlguard_ip=NULL

; intervalo de sondeo para verificar que el extremo del servidor sigue activo (segs)

poll_server_interval=20

; intervalo de sondeo para comprobar el nivel de CPU (segs)

poll_cpu_interval=10

; intervalo de sondeo para comunicar con STAP (segs)

poll_stap_interval=10

; tamaño máximo del archivo de registro del supervisor (KB)

monitor_log_rotate_size=1024

; número de registros rotados del supervisor que conservar

monitor_log_rotate_num_kept=5

; tamaño máximo de los archivos de registro (KB)

log_rotate_size=4096

; número de registros rotados que conservar

log_rotate_num_kept=5

; registros que rotar

logs_to_rotate=/tmp/guard_stap.stderr.txt,/tmp/guard_stap.stdout.txt,/usr/local/guardium/guard_stap/ktap/ktap_install.log,/usr/local/guardium/guard_stap/guard_discovery.stderr.log

; número máximo de interrupciones de STAP por hora (no cuentan las interrupciones resultantes de auto_kill_on_intercept)

kill_num_in_hour=5

; inhabilitar STAP cuando se alcanza el límite de interrupciones por hora o inhabilitar interrupciones y dejar que STAP continúe

; inhabilitar STAP: 1; inhabilitar interrupción: 2

final_action=2

; interrumpir STAP automáticamente en nivel de CPU activado/desactivado (1/0)

auto_kill_on_cpu_enable=0

; nivel de CPU para interrupción (% * 100)

auto_kill_on_cpu_level=8500

; tiempo de espera excedido de snif para interrupción (segs, 0 inhabilitado)

auto_kill_on_snif_timeout=0
```

; tiempo de espera excedido de KTAP para interrupción (segs, 0 inhabilitado)

auto_kill_on_ktap_timeout=0

; tiempo de espera excedido de PCAP para interrupción (segs, 0 inhabilitado)

auto_kill_on_pcap_timeout=0

; tiempo de espera excedido de TEE para interrupción (segs, 0 inhabilitado)

auto_kill_on_tee_timeout=0

; tiempo de espera excedido de SHMEM para interrupción (segs, 0 inhabilitado)

auto_kill_on_shmem_timeout=0

; diagnósticos automáticos activados/desactivados (1/0)

auto_diag=1

; número de ejecuciones de diagnósticos

diag_num=2

; tiempo entre ejecuciones de diagnósticos (mins)

diag_interval=2

; conservar archivos de diag antiguos, sí o no (1/0)

diag_oldrun_saved=0

; interrumpir proceso de STAP después de diags, sí o no (1/0)

diag_auto_kill=0

; nivel de CPU para desencadenar diags (% * 100)

diag_high_cpu_level=7500

; tiempo de espera excedido de snif para desencadenar diags (segs, 0 inhabilitado)

diag_snif_timeout=0

; tiempo de espera excedido de KTAP para desencadenar diags (segs, 0 inhabilitado)

diag_ktap_timeout=0

; tiempo de espera excedido de PCAP para desencadenar diags (segs, 0 inhabilitado)

diag_pcap_timeout=0

; tiempo de espera excedido de TEE para desencadenar diags (segs, 0 inhabilitado)

diag_tee_timeout=0

; tiempo de espera excedido de SHMEM para desencadenar diags (segs, 0 inhabilitado)

diag_shmem_timeout=0

; rastreo automático activado/desactivado (1/0)

auto_trace=0

; tiempo máx para ejecutar rastreo (segs)

trace_max_time=30

; tamaño máximo de archivo de registro para rastreo (MB)

trace_max_log_size=10

; conservar archivos de registro de rastreo antiguos, sí o no (1/0)

trace_oldlog_saved=0

; interrumpir STAP cuando finalicen las ejecuciones de rastreo, sí o no (1/0)

; (es decir, no se cancela debido a CPU baja)

trace_kill_on_complete=0

; nivel de CPU para desencadenar rastreo (% * 100)

trace_high_cpu_level=6000

; nivel de CPU bajo para cancelar rastreo (% * 100)

trace_low_cpu_level=3500

; tiempo de espera excedido para desencadenante de comunicación snif (segs, 0 inhabilitado)

trace_snif_timeout=0

; tiempo de espera excedido para desencadenante de comunicación KTAP (segs, 0 inhabilitado)

trace_ktap_timeout=0

; tiempo de espera excedido de PCAP para desencadenar trace (segs, 0 inhabilitado)

trace_pcap_timeout=0

; tiempo de espera excedido de TEE para desencadenar trace (segs, 0 inhabilitado)

trace_tee_timeout=0

; tiempo de espera excedido de SHMEM para desencadenar trace (segs, 0 inhabilitado)

trace_shmem_timeout=0

; interrumpir STAP automáticamente cuando no se interceptan bases de datos configuradas, sí o no (1/0)

; la característica también se inhabilita si guard_tap.ini muestra que STAP se ejecuta como root

auto_kill_on_intercept=0

; tiempo mínimo entre interrupciones solicitadas por STAP (mins)

intercept_min_time_interval=15

; número máximo de interrupciones de interceptación por hora

intercept_max_num_in_hour=0

Nota: En HP-UX 11.11, la información sobre el mandato de proceso está limitada a 64 caracteres. Esto significa que si la vía de acceso completa al binario de guard_stap tiene más de 64 caracteres, el supervisor de S-TAP no podrá reconocerlo.

Supervisión del comportamiento de S-TAP de Windows

Guardium Agent Monitor (GAM) es un proceso diseñado para supervisar el rendimiento y la capacidad de respuesta del agente Guardium. Se pueden llevar a cabo determinadas acciones en función de diversos umbrales.

Si el agente supervisado supera un umbral configurado, o si no responde a la solicitud de consola (sólo agentes soportados), se pueden realizar las acciones siguientes:

- Ejecutar diag.bat automáticamente
- Iniciar/reiniciar el servicio automáticamente
- Volcar automáticamente el núcleo del servicio

Tabla 2. Qué se supervisa, Windows

Windows
Uso de CPU
Memoria
Manejadores
Número de hebras
"Actividad" - capacidad de respuesta (sólo agentes soportados, actualmente S-TAP es el único agente soportado)

Guardium Agent Monitor se instala junto con S-TAP, pero no se habilita de forma predeterminada.

Nota: Nota: Si se desinstala S-TAP, se desinstalará GAM. Consulte la documentación de instalación de S-TAP para ver detalles.
Nota: Nota: GAM requiere privilegios administrativos.

La ubicación de instalación predeterminada para GAM es la carpeta padre de S-TAP (C:\Program Files\IBM\Guardium Agent Monitor\).

La ubicación predeterminada para la salida de GAM es la subcarpeta \Bin\.

Después de habilitar GAM, asegúrese de que el proceso se ejecuta en el servidor de base de datos (resmon.exe).

Configuración de GAM

Guardium Agent Monitor se ejecuta con su archivo de configuración, resmon.ini, como argumento. El supervisor se controla mediante el archivo resmon.ini.

Configuración global

NUMBER_OF_SERVICES - Número de servicios que se supervisan

UPDATE_INTERVAL - Duración del intervalo entre medidas de sondeo (en segundos)

DEBUG - 1 es para habilitar el registro de depuración de GAM, 0 para no registrar

NUMBER_BYTES_IN_LOG - Número máximo de bytes para el registro de GAM (en KB)

Configuración del umbral de CPU

CPU_LOAD_LIMIT - Porcentaje de umbral de CPU

CPU_INTERVALS_ALLOWED - Número de intervalos que la CPU puede estar por encima del umbral antes de desencadenar una acción (se utiliza junto con UPDATE_INTERVAL para definir un límite de tiempo)

CPUAVE - El valor 1 significa que el porcentaje de CPU es la media entre todos los núcleos de CPU (promedio del sistema)), 0 es el porcentaje del núcleo que utiliza el proceso

Configuración de uso de memoria y de umbrales de recuento de manejadores y de hebras

Para estas medidas hay dos umbrales, límite y límite punta. Una acción se desencadenará cuando se pase un umbral de límite punta o cuando se pase un umbral de límite durante más intervalos de los permitidos.

[METRIC]_LIMIT - Umbral de nivel inferior. Se desencadenará una acción si se pasa durante más intervalos que [METRIC]_INTERVALS_ALLOWED

[METRIC]_PEAK_LIMIT - Umbral de nivel superior. Se desencadenará una acción si se pasa este umbral

[METRIC]_INTERVALS_ALLOWED - Número de intervalos permitidos para el umbral de límite inferior antes de que se desencadene una acción (se utiliza con UPDATE_INTERVAL para el límite de tiempo)

Configuración de acciones

Configuración de acciones

Las configuraciones de acciones se pueden establecer en 0, 1 o 2. 0 significa ninguna acción. 1 significa que el servicio se detendrá y luego se iniciará. 2 significa que el servicio se detendrá.

La segunda y tercera acciones sólo se llevarán a cabo si se desencadenan dentro del ACTION_RESET_INTERVAL de la acción anterior. Transcurrido ACTION_RESET_INTERVAL, la siguiente acción que se debe desencadenará será FIRST_ACTION.

FIRST_ACTION - Lo que se debe hacer la primera vez que se desencadene una acción durante el intervalo

SECOND_ACTION - Lo que se debe hacer la segunda vez que se desencadene una acción durante el intervalo

THIRD_ACTION - Lo que se debe hacer la tercera vez que se desencadene una acción durante el intervalo

ACTION_RESET_INTERVALS - Número de segundos antes de restablecer las acciones

Configuración del volcado de núcleo

Configuración del volcado de núcleo

Se puede realizar un volcado del núcleo siempre que se desencadene una acción estableciendo el valor de ACTION en 1 (en la sección [Global])

ACTION - 1 para realizar un volcado del núcleo cada vez que se desencadena una acción, 0 para no realizar ningún volcado de núcleo

MAX_NUM_DUMP - El número máximo de volcados de núcleo que se guardarán en el directorio de volcado (dump) (conservando el último)

MDTIMEOUT - Tiempo de espera excedido de volcado de núcleo (en milisegundos)

Configuración de diagnósticos

Configuración de diagnósticos

Se puede ejecutar un archivo de diagnósticos siempre que se desencadene una acción estableciendo el valor de DIAGACTION en 1. El script de diagnóstico DIAGNAME que se encuentra en la misma carpeta que la vía de acceso del ejecutable del servicio se ejecutará con los parámetros de DIAG_PARAMETER.

DIAGACTION - 1 para ejecutar el script de diagnóstico siempre que se desencadene una acción 0 para no ejecutar ningún script de diagnóstico

DIAGNAME - Nombre del archivo de diagnóstico que se va a ejecutar (debe estar en la misma carpeta que el ejecutable del servicio)

DIAG_PARAMETER - Parámetros que se utilizarán cuando se ejecute el archivo de diagnóstico

Nota: [METRIC]_INTERVALS_ALLOWED se utiliza junto con UPDATE_INTERVAL para definir un límite de tiempo para el umbral. (Por ejemplo, UPDATE_INTERVAL=1, CPU_INTERVALS_ALLOWED=10, CPU_LOAD_LIMIT=10 significa que se desencadenará una acción si el porcentaje de CPU está por encima del 10% durante más de 10 segundos)

ejemplo de resmon.ini

Ejemplo de resmon.ini

```
;Un signo de punto y coma al principio de la línea indica un comentario

;

[Global]

NUMBER_OF_SERVICES=1

;

;Intervalo para comprobar umbrales (segundos)

UPDATE_INTERVAL=1

;

;Habilita el registro del supervisor

DEBUG=1

;
```

```
;"0" significa que no se realizará un mini volcado para la acción. "1", se realizará un mini volcado
ACTION=1
;
;El número máximo de almacenes de volcado en el directorio de volcado
MAX_NUM_DUMP=3
;
;El tiempo medio de CPU, "0" es un porcentaje de un núcleo, "1" es el porcentaje medio de todos los núcleos del sistema
CPUAVE=1
;
;Tiempo de espera excedido de miniDump en milisegundos
MDTIMEOUT=1000
;Número máximo de BYTES para el registro del supervisor (en KB)
NUMBER_BYTES_IN_LOG=200
;
;Configuración para el servicio
[Service1]
Name=GUARDIUM_STAP
;
;Intervalo para comprobar la actividad (sólo agentes soportados), establecido en "0" para inhabilitar
NAMEDPIPE_INTERVAL=30
;
;Ejecutar diagnóstico sobre acción, establezca en "1" para habilitarlo
DIAGACTION=0
;
;Nombre del archivo de diagnóstico
DIAGNAME=diag.bat
;
;Parámetros de diagnóstico. Si el parámetro tiene espacios, debe escribirse entre comillas
DIAG_PARAMETER=
;
;Porcentaje de límite de cpu
CPU_LOAD_LIMIT=10
;
;Número máximo de intervalos secuenciales sobre CPU_LOAD_LIMIT permitidos
CPU_INTERVALS_ALLOWED=10
;
;Límite de memoria (KB)
MEM_USAGE_LIMIT=150000
MEM_USAGE_PEAK_LIMIT=200000
MEM_USAGE_INTERVALS_ALLOWED=30
;
;Límite de manejadores
HANDLE_COUNT_LIMIT=500
HANDLE_COUNT_PEAK_LIMIT=1000
HANDLE_COUNT_INTERVALS_ALLOWED=20
;
```

```
;Límite de hebras
THREAD_COUNT_LIMIT=200
THREAD_COUNT_PEAK_LIMIT=300
THREAD_COUNT_INTERVALS_ALLOWED=20
;
;'1' emprender acción, luego reiniciar el servicio
;'2' emprender acción, luego detener el servicio sin iniciar
FIRST_ACTION=1
SECOND_ACTION=1
THIRD_ACTION=2
;
;Intervalo de restablecimiento en segundos
ACTION_RESET_INTERVALS=60
```

Tema principal: S-TAPs y otros agentes

Panel de sucesos de S-TAP

Puede utilizar el panel Sucesos S-TAP para ver la salida de los mensajes de sucesos generados por S-TAP.

Para abrir el panel Sucesos de S-TAP para cualquier S-TAP que aparezca en la lista del panel de control:

1. Pulse Informes > Informes operativos de Guardium en tiempo real > Sucesos de S-TAP para abrir Sucesos de S-TAP.

Columna	Descripción
Tipo de suceso	Correcto, Tipo de error, etc.
Descripción del suceso	Brece descripción del suceso
Indicación de fecha y hora	Fecha y hora en que se ha producido el suceso

Nota: Si no se muestra ningún mensaje en el panel Sucesos S-TAP, es posible que se haya inhabilitado la producción de mensajes de sucesos en el archivo de configuración para este S-TAP. Si este es el caso, es posible que pueda localizar los mensajes de sucesos de S-TAP en el sistema host en el archivo de registro de sucesos (para Windows) o en el archivo de registro del sistema (para UNIX/Linux).
Tema principal: S-TAPs y otros agentes

Informes de S-TAP

De forma predeterminada, los informes que se describen en este tema aparecen en el panel Informes.

Puede definir nuevas consultas o informes en el dominio de conexiones inesperadas, y puede crear alertas basadas en excepciones creadas por los S-TAP, pero los demás dominios utilizados por los informes de S-TAP son privados del sistema y los usuarios no pueden acceder a los mismos.

Vista del sistema

Supervisor de estado de S-TAP - Para cada S-TAP que notifica a este sistema Guardium, este informe identifica e l host de S-TAP, la versión de S-TAP, el tipo de servidor de BD, el estado (activo o inactivo), la última respuesta recibida (fecha y hora), el nombre del host primario, e indicadores de tipo true/false para: KTAP, TEE, Memoria compartida de MS SQL Server, Memoria compartida de DB2, Supervisión de TCP local, Uso de conductos con nombre y Cifrado.

Nota: El controlador de memoria compartida de DB2 ha sido reemplazado por la característica Tap de DB2.

Supervisor de tap

Conexiones inesperadas: Este informe solo está disponible cuando la opción Hunter está habilitada en servidores UNIX. La opción Hunter sólo se utiliza cuando se utiliza el método de supervisión Tee. Este informe muestra todos los procesos locales que han evitado S-TAP para conectarse a la base de datos.

Historial de cambios de configuración de S-TAP: Este informe solo se muestra cuando se añade o se modifica un motor de inspección. Muestra los cambios de configuración de S-TAP; cada cambio del motor de inspección se muestra en una fila separada. Cada fila muestra el host de S-TAP, el tipo de servidor de BD, el puerto de BD desde, el puerto de BD hasta, la IP del cliente de BD, la máscara del cliente de BD y la indicación de fecha y hora correspondiente al cambio.

Registro de cambios de host de Guardium primario: Registro de cambios del host primario para los S-TAP. El host primario es el sistema Guardium al que el S-TAP envía los datos. Cada línea del informe muestra el host de S-TAP, el nombre del host de Guardium, el inicio del periodo y el fin del periodo.

Estado de S-TAP: Muestra información de estado sobre cada motor de inspección que se ha definido en cada host de S-TAP. Este informe no tiene parámetros de fecha Desde y Hasta, ya que está informando del estado actual. Cada fila del informe muestra el host de S-TAP, el tipo de servidor de BD, el estado, la última respuesta, el nombre del host primario, indicadores de tipo Sí/No para los siguientes atributos: K-TAP instalado, TEE instalado, Controlador de memoria compartida instalado, Controlador de memoria compartida de DB2 instalado, Controlador de conductos con nombre instalado y Servidor de aplicaciones instalado. Además, muestra el DBS de Hunter.

S-TAP inactivos desde: Muestra todos los S-TAP inactivos definidos en el sistema. Tiene un único parámetro de tiempo de ejecución, QUERY_FROM_DATE, que de forma predeterminada adopta el valor ahora -1 hora. Utilice este parámetro para controlar cómo desea definir *inactivo*. Este informe contiene las mismas columnas de datos que el informe Estado de S-TAP, además de un recuento para cada fila del informe.

Tema principal: S-TAPs y otros agentes

Mensajes de error de S-TAP

En la lista siguiente se describen los mensajes de error que genera S-TAP, en orden alfabético.

Mensaje	Descripción
Cant read inifile .../guard_tap.ini: Cannot resolve hostname xxx for the IP address parameter sqlguard_ip in section SQLGUARD_x. Reverting to .../guard_tap.ini.bak	El archivo de configuración de S-TAP (guard_tap.ini) contiene errores, lo que probablemente se deba a que se ha editado manualmente. Cuando esto sucede, S-TAP intenta reiniciarse desde el último archivo de copia de seguridad correcto conocido (si hay uno disponible).
bind: Address already in use [DB server name or IP] Cant bind listening socket for tee: Address already in use	Un puerto que está intentando utilizar un S-TAP TEE ya se está utilizando. Por ejemplo, si configura un TEE de modo que escuche en el puerto 4100, y Sybase ya escucha en dicho puerto, recibirá este mensaje.
connect: Network is unreachable	El mensaje estándar que se recibe cuando se intenta acceder a un host al que no se puede acceder. En la mayoría de los casos esto significa que el sistema Guardium no está respondiendo a las solicitudes ping.
Delayed server connection error: Connection refused	El sistema Guardium está rechazando una solicitud de conexión procedente de este S-TAP. Ese sistema Guardium no tiene ningún motor de inspección en ejecución (no es probable) o no está configurado para aceptar conexiones de S-TAP (compruebe el valor de unit_type para este sistema Guardium).
Deleting connection on unknown pid:n	No es un mensaje de error; no lo tenga en cuenta.
Got a connection from a remote machine, ignoring	S-TAP ha recibido una solicitud de conexión (a un puerto TEE) desde una aplicación en un host remoto y pasa por alto dicha solicitud. Solo se debe utilizar Tee para conexiones locales.
Got new configuration	El administrador de Guardium ha actualizado la configuración mientras había iniciado sesión en el sistema Guardium y el S-TAP ha recibido el archivo de configuración actualizado.
Guard Tee is accepting connections on port 12346	Mensaje de arranque normal del proceso TEE (solo aparece cuando TEE está instalado).
Guardium TAP starting	Mensaje de arranque normal del proceso S-TAP.
read from socket: Connection reset by peer	El servidor de base de datos o el cliente de base de datos está inactivo. Por ejemplo, alguien ha ejecutado una sesión sqlplus de Oracle y ha utilizado Control-C para salir. Este mensaje no indica un problema.
Server wasn't heard from for 180 sec, closing and re-opening	S-TAP no ha recibido ninguna señal de pulsación desde el sistema Guardium durante 180 segundos. Intentará volver a conectar con el servidor. No se pierden datos ya que se están guardados en el archivo de almacenamiento intermedio.
SQLguard socket read: Connection reset by peer	El sistema Guardium ha cerrado la conexión con el S-TAP. Esto ocurre cuando se reinicia el sistema Guardium o cuando el motor de inspección de sistema Guardium se desactiva automáticamente y se vuelve a activar (en cuyo caso, este mensaje no indica un problema).
waitpid: No child processes	No es un mensaje de error; no lo tenga en cuenta.
killed n	El proceso hunter de S-TAP ha interrumpido una conexión no autorizada identificada por n.

Tema principal: S-TAPs y otros agentes

Apéndice de S-TAP

En esta sección se explica cómo pasar de una versión de Informix a otra.

Procedimiento de transición para pasar de una versión de Informix a otra (SUSE de 32 bits)

Para SUSE de 32 bits Linux, donde hay varias versiones de Informix instaladas, se puede utilizar el siguiente procedimiento paso a paso para pasar de una versión de Informix a otra; el hecho de limpiar semáforos y segmentos de memoria compartida ayuda a garantizar un inicio limpio de la base de datos Informix. En los pasos siguientes se presupone una activación de A-TAP.

1. Mediante el mandato ipcs, obtenga la lista de todos los semáforos y segmentos de memoria compartida que ha creado la base de datos Informix. Esto puede resultar delicado (ya que es posible que aparezcan como pertenecientes al usuario root), pero la regla empírica es que debe haber tres segmentos de memoria compartida con los permisos 0660 y uno con 0666 y cuatro semáforos con permisos 0660 y uno con 0666, todos pertenecientes a root.
2. Detenga la base de datos Informix.
3. Asegúrese de que todos los semáforos y segmentos de memoria compartida creados por la base de datos Informix han desaparecido.
4. (Sólo en Linux) Si la instancia de Informix se ha activado en A-TAP, desactívela.
5. Realice los cambios en /etc/passwd (apunte el directorio de inicio de Informix del usuario a la ubicación correcta).
6. Asegúrese de que el directorio de instalación sea correcto en el motor de inspección de S-TAP para la instancia nueva de Informix. Realice los cambios necesarios y reinicie S-TAP.
7. (Sólo en Linux) Active Informix en A-TAP (asegúrese de especificar la versión correcta).
8. Inicie la nueva instancia.

Tema principal: S-TAPs y otros agentes

Instalación, inicio y detención de CAS desde la línea de mandatos

Utilice los siguientes mandatos para instalar, iniciar y detener CAS.

Puede especificar todos los parámetros necesarios para instalar un CAS de UNIX desde la línea de mandatos.

Sintaxis del script del instalador de línea de mandatos

Estas son las descripciones de cada componente. Las variables se muestran entre corchetes: < >.

```
uso: guard-cas-setup -- install --java-home <JAVA_HOME> --install-path <INSTALL_PATH> --stap-conf <FULL_PATH_TO_GUARD_TAP_INI>

uso: guard-cas-setup -- uninstall
<guard-cas-setup> es el nombre del archivo script
-- install indica una instalación de CAS
-- uninstall indica una desinstalación de CAS
--java-home <JAVA_HOME> identifica el directorio JAVA_HOME. Consulte el apartado sobre cómo obtener información de Java.
--install-path  identifica la vía de acceso de la instalación
--stap-conf <FULL_PATH_TO_GUARD_TAP_INI>identifica la ubicación del archivo guard_tap.ini después de la instalación de un S-TAP.
```

Inicio y detención de CAS

En función del escenario instalación o desinstalación, es posible que tenga que iniciar y detener CAS desde la línea de mandatos. Es posible escenario es que no se suministre la vía de acceso --stap-conf al archivo guard_tap.ini ya que se trata de un parámetro opcional, lo que da como resultado que no se inicie CAS. Utilice los métodos siguientes cuando sea necesario iniciar o detener CAS:

1. Inicie la sesión en el sistema del servidor de base de datos utilizando la cuenta root.
2. Para Red Hat Enterprise Linux 6.
    a. Detenga o inicie CAS mediante los mandatos stop cas o start cas.
3. Todos los demás:
    a. Comente (si se detiene CAS) o elimine el comentario (si se inicia CAS) de la entrada del agente cas en el archivo /etc/inittab. En una instalación predeterminada, esta sentencia se parecerá a la siguiente:

    ```
    cas:<nnnn>::respawn:/usr/local/guardium/guard_stap/cas/bin/run_wrapper.sh /usr/local/guardium/guard_stap/cas/bin
    ```

    b. Guarde el archivo /etc/inittab.
    c. Ejecute el mandato init q
4. Puede validar si CAS se está ejecutando o no mediante la emisión del mandato ps -fe | grep cas.

Tema principal: S-TAPs y otros agentes

Definiciones de IMS

Una definición de IMS establece una conexión entre el sistema Guardium y el entorno de IMS que desea auditar.

Para crear y modificar definiciones de IMS mediante la interfaz del sistema de Guardium, debe haber un S-TAP instalado en el sistema IMS y el espacio de direcciones del agente (AUIASTC) debe tener una conexión preestablecida con el sistema Guardium. Si el agente no se ha conectado correctamente y necesita ayuda para establecer una conexión, consulte el apartado "Instalación de IBM GuardiumS-TAP for IMS on z/OS" en la publicación Guía del usuario de IBM Guardium S-TAP for z/OS.

Una vez definidas, las definiciones de IMS se envían a S-TAP junto con las políticas adicionales de acuerdo con los valores de envío de la política del agente. Las políticas correspondientes a IMS en los S-TAP de z/OS deben estar asociadas a una definición de IMS para que se incluyan durante el envío de políticas. Para obtener más información sobre cómo configurar los sucesos de envío, consulte el tema "Envío de políticas" en la Guía del usuario de IBM Guardium S-TAP for z/OS.

Para obtener soporte paso a paso al configurar definiciones de IMS, consulte el apartado "Creación y modificación de definiciones de IMS" en la Guía del usuario de IBM Guardium S-TAP for z/OS.

Tema principal: S-TAPs y otros agentes

DB2 for i S-TAP

Puede utilizar el S-TAP Guardium DB2 for i para supervisar e informar sobre cualquier acceso a base de datos en IBM i. Esto incluye cualquier programa, como por ejemplo RPG, que utilice operaciones de E/S nativas de base de datos o acceso SQL.

Puede utilizar la información recopilada por el S-TAP Guardium DB2 for i para crear informes de actividad, ayudarle a cumplir los requisitos de auditoría y generar alertas de actividad no autorizada. La información detallada de auditoría incluye:

- Horas de inicio y finalización de sesión
- Puerto y dirección TCP/IP
- Nombres de objeto (por ejemplo, tablas o vistas)
- Usuarios
- SQLSTATE
- Trabajo y números de trabajo
- Variables y sentencias SQL
- Valores especiales de registro de cliente
- Información de interfaz, como por ejemplo ODBC, ToolboxJDBC, Native JDBC, .NET, etc.

El S-TAP recibe datos de dos orígenes:

- Datos de SQL Performance Monitor (también conocido como supervisor de base de datos) para aplicaciones SQL
- Entradas de auditoría procedentes del diario de auditoría QSYS/QAUDJRN para aplicaciones que utilizan interfaces que no son SQL

Los datos procedentes de estos orígenes incluyen:

- Cualquier acceso SQL, tanto si se ha iniciado en el servidor de IBM i como si se ha iniciado desde un cliente
- Cualquier acceso nativo que se capture en el diario de auditoría

El S-TAP envía estos datos al sistema Guardium en tiempo real.
Para obtener más información sobre el S-TAP de DB2 for i y temas relacionados, consulte estas fuentes:

- Utilización de IBM Security Guardium para supervisión y auditoría de la actividad de la base de datos IBM DB2 for i: este artículo de developerWorks contiene una introducción a IBM Guardium, el STAP de DB2 for i, y detalles relacionados con las claves.
- IBM i on IBM Knowledge Center: consúltelo para obtener información sobre IBM i, diario de auditoría y otros tremas relacionados.

S-TAP i para cifrado, equilibrio de carga y sustitución por anomalía

El S-TAP IBM i da soporte al cifrado TLS y al equilibrio de carga y sustitución por anomalía de sesiones de S-TAP.

Nota: El soporte de S-TAP TLS y equilibrio de carga solo se admite en IBM i 7.1 y 7.2.

Al igual que los S-TAP UNIX, los parámetros de configuración de S-TAP i se guardan en un archivo guard_tap.ini en el directorio /usr/local/guardium del servidor IBM i.

Los administradores configuran el S-TAP mediante las mismas API e IU (Control de S-TAP) que otros S-TAPS de UNIX. Cuando se utiliza la GUI o API para realizar un cambio en la configuración S-TAP, el componente sniffer de Guardium envía un mensaje al S-TAP, el cual hace una copia de seguridad del archivo .ini antiguo, guarda la configuración en el nuevo archivo .ini y luego se reinicia.

Los administradores pueden configurar la comunicación cifrada entre el S-TAP y el dispositivo mediante los controles de configuración de S-TAP y pueden configurar diversas opciones de equilibrio de carga.

Utilización del equilibrio de carga y la sustitución por anomalía de S-TAP

Las opciones de sustitución por anomalía y equilibrio de carga de i S-TAP son similares a las de los S-TAP de UNIX. Utilice el parámetro participate_in_load_balancing para determinar si se debe utilizar el comportamiento de sustitución por anomalía o equilibrio de carga. Utilice las secciones de SQLGuard del S-TAP para configurar los hosts Guardium primario, secundario y terciario.

Una diferencia es que no se necesita participate_in_load_balancing=3; debido a la forma en que está diseñada la comunicación I S-TAP, la información de sesión completa está disponible en cada mensaje. Esto significa que, incluso antes de las mejoras proporcionadas en este parche, podría utilizar el equilibrio de hardware (por ejemplo F5) con participate_in_load_1 y una dirección IP virtual en la sección de SQLGuard primaria del archivo de configuración.

En una configuración de sustitución por anomalía, el S-TAP está configurado para registrarse con varios recopiladores, pero para enviar el tráfico solamente a un recopilador cada vez (participate_in_load_balancing=0). El S-TAP de esta configuración envía todo su tráfico a un recopilador, a menos que encuentre problemas de conectividad con dicho recopilador que desencadene una sustitución por anomalía a un recopilador secundario.

Cómo utilizar AppEvent de IMS

Los datos que contienen la información de usuario de una llamada DLI APP_EVENT deben tener una sintaxis similar a la de la api GuardAppEvent.

Los dos primeros bytes representan el ccsid de la codificación de los bytes siguientes. Por ejemplo, 0x04B8 significa ccsid 1208. Los bytes siguientes deben tener la sintaxis tal como se indica a continuación:

SELECT

'GuardAppEvent:Start',

'GuardAppEventType:type',

'GuardAppEventUserName:name',

'GuardAppEventStrValue:string',

'GuardAppEventNumValue:number',

'GuardAppEventDateValue:date'

FROM DUAL

Para obtener más información sobre tipo, nombre, serie, número y fecha, consulte la API de GuardAppEvent.

Actualmente solo se da soporte a la codificación UTF8.

- Estrategia de supervisión
  Para que su sistema de supervisión y auditoría sea eficaz y eficiente, desarrolle una estrategia que reconozca y cumpla con sus requisitos.
- Instalación del S-TAP para IBM i
  Siga estos pasos para instalar o desinstalar el S-TAP.
- Definición del S-TAP para IBM i
  Después de instalar el S-TAP, asegúrese de que se puede comunicar con el sistema Guardium.

Tema principal: S-TAPs y otros agentes

Estrategia de supervisión

Para que su sistema de supervisión y auditoría sea eficaz y eficiente, desarrolle una estrategia que reconozca y cumpla con sus requisitos.

Cuando sepa los datos que necesita, desarrolle una estrategia para recopilarlos con la menor cantidad posible de datos superfluos. La supervisión y registro de datos que no necesita aumenta el uso de espacio de disco y de potencia de proceso y generan tráfico de red adicional. Existen varias áreas en las que puede implementar su estrategia:

Supervisión de bases de datos

El supervisor de SQL global captura información de SQL y la coloca en una cola para el S-TAP. Puede utilizar las funciones de filtrado del supervisor para controlar los tipos de usuarios y objetos que se colocan en cola. De forma predeterminada, estos tipos de entradas no se reenvían desde S-TAP al sistema Guardium:

Abreviatura de SQL	Significado
AD	ALLOCATE DESCRIPTOR
CL	CLOSE
DA	DEALLOCATE DESCRIPTOR
DE	DESCRIBE
EX	EXECUTE (se audita la sentencia ejecutada de SQL)
FE	FETCH

FL	FREE LOCATOR
GD	GET DIAGNOSTICS
GS	GET DESCRIPTOR
HL	HOLD LOCATOR
PR	PREPARE (except authorization errors are captured)
RE	RELEASE
RG	RESIGNAL
SC	SET CONNECTION
SD	SET DESCRIPTOR
SG	SIGNAL

Diario de auditoría

Puede configurar el diario de auditoría del sistema para que solo capture aquellas entradas relacionadas con los objetos o los usuarios que le interesen. De forma predeterminada, las entradas de estos tipos se envían desde el S-TAP al sistema Guardium:

Abreviatura de SQL	**Significado**
ZR	Leer objeto
ZC	Cambiar objeto
CA	Cambio de autoridad
AD	Cambio de auditoría
AF	Error de autoridad
CO	Crear objeto
DO	Suprimir objeto
SV	Cambio de valor del sistema
GR	Registro de auditoría de finalidad general
OM	Objeto movido o redenominado
PG	Cambio de grupo primario
PW	Contraseña o ID de usuario no válido
OW	Cambiar propietario
OR	Objeto restaurado
RA	Restaurar cambio de autoridad
RO	Restaurar cambio de propietario
RZ	Restaurar cambio de grupo primario

Solo se reenvían las entradas relacionadas con los objetos de la base de datos:

- *FILE (una tabla, vista, índice, archivo lógico, alias o archivo de dispositivo)
- *SQLUDT (un tipo definido por usuario de SQL)
- *SQLPKG (un paquete de SQL)
- *PGM (un procedimiento, función o programa)
- *SRVPGM (un procedimiento, función, variable global o programa de servicio)
- *DTAARA (una secuencia de SQL)

En el sistema Guardium

Puede definir políticas que controlen qué información recibida del S-TAP se ignora y qué acciones se deben realizar en función de otros elementos.

El hecho de pasar por alto datos una vez que se han enviado sobre través de la red resulta ineficaz. Siempre que sea posible, filtre la información que no necesite antes de que se coloque en la cola del S-TAP.

Tema principal: DB2 for i S-TAP

Instalación del S-TAP para IBM i

Siga estos pasos para instalar o desinstalar el S-TAP.

Antes de empezar

El S-TAP de DB2 para i requiere Portable Application Solutions Environment (PASE), que se inicia y se detiene automáticamente según sea necesario cuando un usuario inicia y detiene el S-TAP de DB2 for i desde la interfaz de usuario de IBM Guardium.

Debe conocer la dirección IP del sistema Guardium al que se conectará este S-TAP.

Cuando descargue el S-TAP, asegúrese de filtrar por la plataforma IBM i, para asegurarse de que descarga el paquete correcto.

Acerca de esta tarea

Guardium Installation Manager (GIM) no recibe soporte en IBM i.

Puede utilizar el software de emulador de 5250 para conectarse de forma remota al sistema IBM i.

Procedimiento

1. En el servidor IBM i, especifique este mandato para abrir el shell PASE: call qp2term.
2. En el entorno de shell PASE, cree un directorio temporal para que contenga el script de instalación de S-TAP, como por ejemplo /tmp.
3. Utilice FTP para mover el siguiente script de shell de instalación de S-TAP a dicho directorio temporal: guard-itap-9.0.0_*rnnnnn*-aix-5.3-aix-powerpc.sh
4. En el mismo directorio, ejecute este mandato:

   ```
   guard-itap-9.0.0_rnnnnn-aix-5.3-aix-powerpc.sh guardium_host_IP
   ```

   donde *guardium_host_IP* es la dirección IP del sistema Guardium.

Resultados

El S-TAP se instala en /usr/local/guardium. Una vez finalizada la instalación, el S-TAP intenta iniciar los procesos que habilitan la supervisión de actividad y conectarse al sistema Guardium utilizando la dirección IP que se ha especificado con el mandato de instalación.

Qué hacer a continuación

Para comprobar que la instalación se ha realizado correctamente e iniciar el proceso de auditoría, inicie una sesión en la consola web de IBM Guardium como administrador, vaya al separador Vista del sistema y compruebe el estado del S-TAP.

Tema principal: DB2 for i S-TAP

Desinstalación del S-TAP

Procedimiento

Para detener y desinstalar el S-TAP, emita estos mandatos:

```
RUNSQL SQL('call SYSPROC/SYSAUDIT_End') COMMIT(*NONE)
RMVDIR DIR('/usr/local/guardium') SUBTREE(*ALL)
```

Definición del S-TAP para IBM i

Después de instalar el S-TAP, asegúrese de que se puede comunicar con el sistema Guardium.

Antes de empezar

Debe conocer las credenciales de inicio de sesión para el sistema IBM i.

Acerca de esta tarea

Los pasos principales para configurar el S-TAP son:

1. Defina DB2 para i como un origen de datos reconocido para IBM Guardium y pruebe la conexión.
2. Llene el sistema Guardium con información del archivo de configuración de IBM i que se creó al instalar el S-TAP de DB2 para i, utilizando el proceso del Generador de tablas personalizadas.
3. Cree un informe de configuración de DB2 para i. Desde esta interfaz de informe puede invocar las API de Guardium que le permiten iniciar y detener el proceso de supervisión, obtener información de estado y actualizar los parámetros de configuración, incluidos los valores de filtrado.

Procedimiento

1. Pulse Configuración > Herramientas y vistas > Definiciones de orígenes de datos para abrir el Creador de orígenes de datos. Seleccione Dominio personalizado en el recuadro de selección de aplicaciones. Pulse Siguiente.
2. En el Buscador de orígenes de datos, pulse Nuevo, lo que abrirá el Creador de orígenes de datos.
3. Seleccione DB2 para i como Tipo de base de datos y, a continuación, añada la información adecuada para el host, nombre de servicio y credenciales. Pulse Aplicar.
4. Pulse Probar conexión para asegurarse de que la configuración se ha realizado correctamente.
5. Pulse Herramientas > Creador de informes.
6. Pulse Creador de tablas personalizadas. Seleccione Configuración de S-TAP de DB2 para i y a pulse Subir datos. El Buscador de orígenes de datos muestra una lista de los S-TAP de DB2 para i.
7. Seleccione su origen de datos de DB2 para i en la lista y pulse Añadir.
8. En la pantalla Importar datos, asegúrese de que aparezca el origen de datos de DB2 para i. Pulse Aplicar y luego pulse Ejecutar una vez ahora. Debería ver un mensaje que indique que la operación ha finalizado correctamente con una fila insertada.
9. Pulse Personalizar en la barra de título de Guardium. Luego pulse Añadir panel.
10. Asigne un nombre nuevo al panel, como por ejemplo Mis informes nuevos y pulse Aplicar.
11. Mis informes nuevos aparece en el panel Personalizar. Pulse el icono situado junto al nombre. En la lista desplegable Diseño, seleccione Panel de menú. Pulse Guardar. El nuevo panel aparece como un separador.
12. Pulse Creación de informes en el panel de navegación.
13. En la lista desplegable de consultas, pulse Configuración de S-TAP de DB2 para i y luego pulse Buscar.
14. Busque la configuración de S-TAP de DB2 para i y pulse Añadir a Mis informes nuevos (o el nombre que haya especificado en el paso 10).
15. Abra el separador Mis informes, que ahora muestra la fila del informe de IBM i. Efectúe una doble pulsación en una fila del informe y seleccione Invocar. Se visualiza una lista de las API de IBM Guardium que puede seleccionar.
16. Seleccione update_istap_config.
17. Cuando se selecciona una API de Guardium, se muestran los parámetros de dicha API. Puede cambiar los valores que necesite. Cambie el valor del parámetro start_monitor por 1. Pulse Invocar ahora.

Resultados

Utilizando los datos que ha especificado, la API update_istap_config realiza estas tareas:

- Crea la cola de mensajes que se utilizará para enviar entradas desde el S-TAP al sistema Guardium e inicia un supervisor de base de datos global utilizando una vista con un desencadenante INSTEAD OF, que envía las entradas a la cola de mensajes.
- Inicia PASE y el S-TAP.
- Recibe entradas de diario de QAUDJRN y las añade a la cola de mensajes.

Tema principal: DB2 for i S-TAP

IBM Security Guardium S-TAP for z/OS

La solución IBM Security Guardium S-TAP for z/OS es una herramienta que recopila y correlaciona información de acceso a datos para DB2 en z/OS, Data Sets en z/OS o IMS en z/OS para generar una vista completa de la actividad empresarial para los auditores.

IBM Security Guardium S-TAP for DB2 on z/OS

S-TAP for DB2 on z/OS recopila y correlaciona información de acceso a datos de diversos recursos de DB2 para generar una vista completa de la actividad empresarial para los auditores. S-TAP for DB2 on z/OS captura el tráfico de la base de datos DB2/zOS y lo reenvía al sistema Guardium. El tráfico que captura S-TAP for z/OS se reenvía directamente al sistema Guardium, donde se pueden utilizar políticas en tiempo real. Guardium proporciona las siguientes características y funciones:

- Recopilación de datos: Guardium puede recopilar y correlacionar muchos tipos diferentes de información en un repositorio de administración:
  - Modificaciones de un objeto (SQL UPDATE, INSERT, DELETE)
  - Lecturas de un objeto (SQL SELECT)
  - Operaciones explícitas GRANT y REVOKE (para capturar sucesos en los que los usuarios pueden estar intentando modificar niveles de autorización)
  - Asignación o modificación de un ID de autorización
  - Intentos de autorización que se deniegan debido a una autorización inadecuada
  - Operaciones CREATE, ALTER y DROP sobre un objeto (por ejemplo, una tabla)
  - Acceso de programa de utilidad a un objeto (sólo programas de utilidad de IBM®).
  - Mandatos de DB2 especificados (incluida la capacidad para determinar qué usuarios están emitiendo mandatos específicos)
- Interfaz de usuario de administración: facilita a los administradores del producto la configuración de consultas de datos.

Nota: Para DB2 on z/OS, dentro de los informes, el programa fuente tal como se ha definido en la entidad de cliente/servidor será la concatenación del nombre del servidor y el ID de correlación.
Nota: Para DB2 on z/OS, para utilizar DB2 Unicode Database y mostrar los caracteres de varios bytes correctamente en los informes, cambie el parámetro de DB2 UIFCIDS de No a Yes.

IBM Security Guardium S-TAP for Data Sets on z/OS

S-TAP for Data Sets on z/OS es una herramienta que recopila y correlaciona información de acceso a datos de los registros para generar una vista completa de la actividad empresarial para los auditores. S-TAP proporciona las siguientes características y funciones:

- Recopilación de datos: S-TAP puede recopilar y correlacionar muchos tipos diferentes de información:
  - SMF registra el acceso a los conjuntos de datos de Data Sets y las infracciones de seguridad.
  - Operaciones de conjuntos de datos realizadas en los conjuntos de datos de Data Sets, como supresiones o cambios de nombre.

IBM Security GuardiumS-TAP for IMS on z/OS

S-TAP for IMS on z/OS es una herramienta que recopila y correlaciona información de acceso a datos de regiones en línea de IMS, trabajos por lotes de IMS, conjuntos de datos de registro archivados de IMS y registros de SMF para generar una vista completa de la actividad empresarial para los auditores. IBM Guardium S-TAP proporciona las siguientes características y funciones:

- Recopilación de datos: S-TAP puede recopilar y correlacionar muchos tipos diferentes de información:
  - Accesos a bases de datos y segmentos desde regiones en línea de IMS.
  - Acceda a bases de datos y segmentos desde trabajos por lotes DLI/DBB de IMS.
  - Acceso a la base de datos, copia de imagen y conjuntos de datos RECON e infracciones de seguridad registradas por SMF.
  - INICIO y DETENCIÓN de la región en línea de IMS, cambio de actividad de estado de base de datos y PSB e inicio y finalización de sesión de USUARIO, según los datos registrados en los conjuntos de datos del registro de archivado de IMS.
- Interfaz de usuario de administración: proporciona a los auditores opciones flexibles para la gestión y auditoría de perfiles.

Nota: No se da soporte a ninguna acción de bloqueo ni a reglas de extrusión. Restricción: S-TAP for IMS da soporte a la auditoría de bases de datos de entrada de datos (DEDB) y de bases de datos de función completa de IMS. No se da soporte a la auditoría de bases de datos de almacenamiento principal (MSDB)

IBM Security Guardium S-TAP for z/OS

Se presupone que el cliente S-TAP para z/OS está instalado y configurado para capturar tráfico.

Para obtener información adicional, consulte las siguientes Guías de usuario. Estas Guías de usuario contienen información acerca de Guardium S-TAP; proporcionan una visión general y sus funciones, así como tareas para planificar, instalar, configurar y utilizar Guardium.

Las Guías de usuario disponibles son:

- IBM Security Guardium S-TAP for DB2 on z/OS
- IBM Security Guardium S-TAP for Data Sets on z/OS
- IBM Security GuardiumS-TAP for IMS on z/OS

Nota: Encontrará las versiones actuales de estas guías en Guardium Knowledgecenter, http://www.ibm.com/support/knowledgecenter/SSMPHH/SSMPHH_welcome.html

Imposición de políticas

Consulte lo siguiente:

S-TAP for IMS: http://www.ibm.com/support/knowledgecenter/SSMPHH_10.1.0/com.ibm.guardium.doc.zos/AUI/auiur061.html

S-TAP for DB2: http://www.ibm.com/support/knowledgecenter/SSMPHH_10.1.0/com.ibm.guardium.doc.zos/ADH/adhuc007.html

S-TAP for Data Sets: http://www.ibm.com/support/knowledgecenter/SSMPHH_10.1.0/com.ibm.guardium.doc.zos/AUV/auvur021.html

Definición de la interfaz de Guardium for z/OS

Utilice la pantalla Definiciones para mantener uno o varios servidores de los que se deben recuperar los archivos de z/OS.

1. Seleccione Configurar > Herramientas y vistas > Guardium for z/OS.
2. Pulse el botón Nuevo para crear una nueva interfaz de Guardium for z/OS o seleccione una interfaz existente en el buscador de definición de interfaz de Guardium for z/OS para suprimirla, modificarla o realizar un comentario sobre la misma.
3. En el recuadro IP de servidor, especifique la dirección IP que utilizará la interfaz de Guardium for z/OS para recuperar archivos.
4. En el recuadro Nombre de servidor, especifique el Nombre de servidor que utilizará la interfaz de Guardium z/OS para recuperar los archivos.
5. En el recuadro Directorio, especifique el directorio en el que se encuentran los archivos de auditoría de z/OS.
6. En los recuadros Usuario y Contraseña, especifique un nombre y una contraseña que se utilizarán para acceder a los servidores FTP/SFTP para extraer (y suprimir) los archivos de z/OS.
7. En el recuadro SSID, especifique el SSID del servidor de base de datos.
8. En el recuadro Sufijos de archivo, especifique las extensiones de archivo apropiadas separadas por comas. Consulte Equilibrio de carga para obtener información adicional.
9. En el recuadro Método de transferencia, seleccione FTP o SFTP.
10. Marque Utilizar END_USER_ID para el nombre de usuario de aplicación si la aplicación ha proporcionado información de app_user; de lo contrario, el tráfico entre la aplicación y la base de datos no contendrá esta información. Es decir, esto indica al analizador qué debe esperar en los campos de información de app_user (correlación end_user_identity).
11. Marque o desmarque el recuadro Activo para activar o desactivar esta interfaz
12. Marque el recuadro Eliminar archivos para eliminar archivos del servidor después de que se transfiera el archivo. Es muy recomendable que se establezca en Eliminar archivos para evitar que se acumulen demasiados archivos y se produzcan problemas de espacio de disco.
13. Pulse el botón Aplicar para guardar esta configuración.

Nota: Esta pantalla del menú de definición de la interfaz de Guardium for z/OS contiene sugerencias para determinadas opciones de menú. Mueva el cursor sobre una opción de menú (como por ejemplo Directorio) y aparecerá una descripción breve.
Nota: Cuando se edita una definición existente, si la entrada de usuario de la contraseña está vacía, se conserva la contraseña anterior. Cuando se añade un registro nuevo, se debe especificar el nombre de usuario y la contraseña.

Configuración de origen de datos de conexión SSL de DB2 for z/OS

Requisitos: en el lado del servidor del sistema principal de DB2 for z/OS, el administrador de base de datos deberá configurar SSL y establecer el rol de reconocimiento en una de las opciones siguientes y proporcionar un certificado de cliente en formato PEM que deberá cargarse en la configuración del origen de datos:

1. HandShakeRole ServerWithClientAuth
2. HandShakeRole Server

Cumplimente la pantalla de menú Actualizar origen de datos con estas selecciones:

1. Para Tipo de aplicación, seleccione Asesoramiento de seguridad.
2. En Nombre, especifique el nombre que desee para el origen de datos.
3. Para Tipo de base de datos, seleccione DB2 for z/OS.
4. En Descripción, escriba la descripción que desee para el origen de datos.
5. Marque el recuadro Utilizar SSL y, después de pulsar el recuadro Utilizar SSL, tendrá que pulsar el botón Añadir certificado y subir el archivo PEM proporcionado por el DBA de DB2 for z/OS.
6. Pulse Importar certificado ssl del servidor.
7. Para Autenticación, marque Asignar credenciales y especifique lo siguiente:
    a. En Nombre de usuario, especifique el usuario de DB2 z/OS.
    b. En Contraseña, escriba la contraseña del usuario de DB2 z/OS.
    c. En Nombre de host/IP, especifique el Nombre de host o la IP de la instancia de DB2 z/OS.
    d. En Nombre de base de datos, escriba el nombre de la base de datos DB2 z/OS.
    e. En Número de puerto, escriba el número de puerto para la base de datos DB2 z/OS.

Nota: La propiedad Connection de sslConnection=true está codificada para facilitar el uso para el usuario final.

Soporte de juegos de caracteres

Para valores de variables de host, se pueden utilizar distintos identificadores de juegos de caracteres codificados (CSSID), algunos de los cuales reciben soporte y otros no.

- En el caso de CSSID soportados, las variables se convertirán consecuentemente
- En el caso de CSSID no soportados, las variables se representarán mediante una concatenación de CSSID y el valor no convertido, como: CSSID [número_de_CSSID] : xxxxxxxxxxxxx donde x será el valor no convertido, tal como se ha recibido del archivo.

Juegos de caracteres no soportados

- MacCE
- Cp853

Guardium Installation Manager

Puede utilizar Guardium Installation Manager (GIM) para instalar y mantener componentes de Guardium en servidores gestionados.

El componente GIM incluye un servidor GIM, que se instala como parte del sistema Guardium, y un cliente GIM, que debe estar instalado en los servidores que alojan las bases de datos o los sistemas de archivos que desea supervisar. El cliente GIM es un conjunto de scripts Perl que se ejecutan en cada servidor gestionado. Después de instalar el cliente GIM, trabajar con el servidor GIM para realizar estas tareas:

- Comprobar si hay actualizaciones del software instalado
- Transferir e instalar software nuevo
- Desinstalar software
- Actualizar parámetros de software
- Supervisar y detener procesos que se ejecutan en el servidor de base de datos

Por ejemplo, puede utilizar GIM para instalar módulos de S-TAP y mantenerlos actualizados.

El cliente GIM utiliza el puerto 8444 para comunicarse con el servidor GIM.

Puede utilizar el servidor GIM a través de la interfaz de usuario de Guardium o a través de la interfaz de línea de mandatos (CLI).

Los módulos de software que puede desplegar mediante GIM están empaquetados como lote de GIM. Un *lote* es un archivo de tipo gim que contiene software que se puede desplegar mediante GIM.

Si el entorno incluye un sistema Guardium que está configurado como un gestor central, debe decidir qué sistemas Guardium desea utilizar como servidores GIM. Puede gestionar todos los clientes GIM, con un máximo de 4000, desde un solo sistema Guardium, como el gestor central, o los puede gestionar en grupos desde distintos sistemas Guardium. Si gestiona todos los clientes GIM desde un único sistema Guardium, puede ver el estado de todos los clientes GIM y realizar tareas relacionadas desde esta interfaz de usuario única. Si opta por gestionar los clientes GIM en grupos desde distintos sistemas Guardium, puede utilizar cada interfaz de usuario para trabajar con los clientes GIM que gestiona; no dispondrá de ninguna vista general.

Si actualiza a la Versión 10.0 desde V9.0 GPU parche 50 o posterior, no hay ningún cambio en la forma en que puede ver información sobre los clientes GIM. Si actualiza desde una versión anterior, se aplican estas restricciones: después de actualizar el gestor central, puede seguir viendo información sobre los clientes GIM que están asignados a otros sistemas Guardium, pero no puede realizar el suministro a esos clientes GIM desde el gestor central. Después de actualizar todos los sistemas Guardium, solo puede ver cada cliente GIM desde el sistema Guardium que es su servidor GIM.

Para gestionar un gran número de instalaciones de GIM, puede crear grupos de clientes GIM. Luego puede utilizar los grupos para instalar, actualizar y gestionar lotes de software.

El cliente GIM supervisa los procesos que se instalan mediante GIM. Comprueba el latido de cada proceso una vez por minuto y pasa los cambios de estado correspondientes a los procesos al servidor GIM. El estado de cada proceso se visualiza en el panel Supervisión de procesos. Los cambios quedan reflejados en tres minutos. Los cambios en el estado del propio cliente GIM quedan reflejados según el intervalo en el que el cliente sondea el servidor y distribuye su "mensaje alive".

Nota: Cuando se realiza una copia de seguridad y restauración del sistema desde un servidor, que tiene GIM definido, a otro servidor, el usuario debe configurar una sustitución por anomalía de GIM en el servidor de restauración. Esta configuración de GIM se aplica a un gestor central de copia de seguridad o a una copia de seguridad y restauración del sistema.

- Inicio rápido para desplegar agentes de supervisión
  Utilice la herramienta Desplegar agentes de supervisión para activar automáticamente clientes GIM, instalar S-TAP y empezar a supervisar el tráfico de base de datos.
- Gestión de software con GIM
- Asignación de servidores GIM
  Se puede conectar de forma remota a un agente GIM preinstalado e inactivo (no conectado a ningún recopilador) y hacer que se conecte a algún recopilador sin necesidad de acceder al servidor de base de datos.
- Instalación del cliente GIM en un servidor Windows
  Obtenga información sobre cómo instalar el cliente GIM para Windows mediante un instalador interactivo o una instalación silenciosa. También encontrará instrucciones para desinstalar el cliente GIM.
- Instalación del cliente GIM en un servidor UNIX
  Utilice este mandato para instalar el cliente GIM en cada servidor de base de datos.
- Actualización del cliente GIM
  Puede utilizar GIM para actualizar el cliente GIM a una versión más reciente.
- Utilización de grupos con GIM
  Puede utilizar grupos para facilitar algunas tareas de GIM.
- Cómo copiar un módulo K-TAP mediante GIM
  Si crea un módulo K-TAP personalizado para un servidor de base de datos Linux, puede utilizar GIM para copiar dicho módulo en otros servidores de base de datos Linux.
- Actualización dinámica de GIM
  Los clientes GIM comprueban si hay actualizaciones del servidor GIM a intervalos regulares. El servidor GIM puede calcular el mejor intervalo de sondeo a utilizar en función de las condiciones del sistema.
- Cuando actualice el sistema operativo del servidor de base de datos
  Cuando actualice el sistema operativo del servidor de base de datos, puede dejar que el cliente GIM realice los cambios necesarios en sí mismo y en los módulos instalados por GIM.
- Distribución de lotes de GIM a unidades gestionadas
  Puede distribuir lotes de GIM a unidades gestionadas para desplegarlos en los clientes GIM gestionados por dichas unidades gestionadas.
- Eliminación de lotes de GIM no utilizados
  Puede eliminar los lotes de GIM del servidor GIM si ya no se utilizan en ningún servidor de base de datos.
- Ejecución de diagnósticos de GIM
  Puede ejecutar diagnósticos en los clientes GIM para verificar que el servidor GIM tiene datos exactos sobre cada cliente.
- Depuración de operaciones de GIM
  Es posible que tenga que activar la depuración para resolver un problema.
- Reinicio del supervisor para Solaris con soporte de SMF
  Utilice un conjunto de mandatos de la CLI para reiniciar el supervisor en servidores Solaris con soporte de SMF.

Inicio rápido para desplegar agentes de supervisión

Utilice la herramienta Desplegar agentes de supervisión para activar automáticamente clientes GIM, instalar S-TAP y empezar a supervisar el tráfico de base de datos.

La herramienta para desplegar agentes de supervisión simplifica el proceso de establecer un despliegue de Guardium. Basada en la infraestructura existente de Guardium Installation Manager (GIM), la herramienta para desplegar agentes de supervisión le ayuda a encontrar rápidamente servidores de bases de datos, a instalar agentes de supervisión (S-TAP) y a configurar motores de inspección para sus bases de datos. Además, la herramienta ofrece una vista centralizada para realizar un seguimiento y revisar el estado del despliegue.

- Requisitos previos para desplegar agentes de supervisión
  Revise los requisitos previos y las restricciones antes de empezar a desplegar agentes de supervisión.
- Desplegar agentes de supervisión
  Aprenda cómo desplegar rápidamente S-TAP y cómo configurar motores de inspección.

Tema principal: Guardium Installation Manager

Requisitos previos para desplegar agentes de supervisión

Revise los requisitos previos y las restricciones antes de empezar a desplegar agentes de supervisión.

Antes de utilizar la herramienta de despliegue de agentes de supervisión para instalar S-TAP y configurar motores de inspección en los servidores de base de datos, compruebe los siguientes requisitos previos.

Instale los clientes GIM en modalidad de escucha

Instale los clientes GIM en modalidad de escucha en uno o varios servidores de base de datos del entorno. Para instalar el cliente GIM en modalidad de escucha en sistemas Windows, omita el parámetro `--host`. Para instalar el cliente GIM en modalidad de escucha en sistemas como AIX y Linux, omita el parámetro `--sqlguardip`. Para obtener más información sobre la modalidad de escucha de GIM, consulte Asignación de servidores GIM.
Importante: Es posible que tenga que abrir un puerto entre el cliente GIM en el servidor de base de datos y el sistema Guardium en el que va a ejecutar la herramienta de despliegue de agentes de supervisión. Se utiliza el puerto predeterminado 8445 a no ser que especifique otro puerto al instalar el cliente GIM.

Cargue los módulos GIM S-TAP en el sistema Guardium

Ejecute la herramienta de despliegue de agentes de supervisión como usuario administrativa desde cualquier sistemas Guardium que no esté configurado como agregador. Antes de empezar, siga el siguiente procedimiento para cargar los módulos GIM S-TAP en el sistema Guardium.

1. Vaya a Gestionar > Instalación de módulo > Cargar módulos.
2. Pulse Elegir archivo y seleccione el módulo que desea instalar.
3. Pulse Cargar para cargar el módulo en el sistema Guardium. Después de cargarlo, el módulo aparecerá en la lista de la tabla Importar módulos subidos table.
4. En la tabla Importar módulos subidos, marque el recuadro de selección que hay junto al módulo que desea instalar. El módulo se importará y estará listo para su instalación. Una vez importado el módulo, se volverá a cargar la página Subir módulos y el módulo dejará de aparecer en la tabla Importar módulos subidos.

Para obtener información sobre las ofertas S-TAP y plataformas soportadas, consulte Requisitos del sistema y plataformas soportadas para IBM Security Guardium.

Compruebe que todos los servidores de base de datos que se pueden descubrir se están ejecutando

Los motores de inspección se pueden configurar automáticamente para algunas bases de datos, incluidas las siguientes:

- DB2 para Linux, UNIX y Windows
- Informix
- Microsoft SQL Server
- MySQL
- Oracle
- Postgre SQL
- Sybase
- Teradata

Para permitir la configuración automática de los motores de inspección, compruebe que los servidores de base de datos se estén ejecutando antes de desplegar los agentes de supervisión.

Para obtener más información sobre cómo descubrir automáticamente instancias de base de datos, consulte S-TAP Discovery.

Tema principal: Inicio rápido para desplegar agentes de supervisión

Desplegar agentes de supervisión

Aprenda cómo desplegar rápidamente S-TAP y cómo configurar motores de inspección.

Antes de empezar

Ejecute la herramienta de despliegue de agentes de supervisión como usuario administrativa desde cualquier sistemas Guardium que no esté configurado como agregador. Antes de empezar, verifique lo siguiente:

- Los clientes GIM están instalados en modalidad de escucha.
- Los módulos GIM S-TAP se han importado al sistema Guardium.
- Se están ejecutando los servidores de base de datos que se pueden descubrir.

Para obtener más información, consulte Requisitos previos para desplegar agentes de supervisión.

Acerca de esta tarea

En el siguiente procedimiento se describe cómo utilizar la herramienta para desplegar agentes de supervisión para instalar rápidamente S-TAP y configurar motores de inspección para supervisar el tráfico de base de datos.

Procedimiento

1. Para abrir la herramienta para desplegar agentes de supervisión, vaya a Configurar > Inicio rápido > Desplegar agentes de supervisión.
2. En la sección Identificar servidores de base de datos, utilice el campo Direcciones IP para especificar el rango de direcciones IP para buscar clientes GIM en modalidad de escucha. Utilice el icono para especificar direcciones IP adicionales. Si desea expandir la búsqueda, incluya caracteres comodín (`*`) o caracteres de rango (`-`). Por ejemplo, `10.0.0-5.*`.
   Importante: Se tarda mucho en escanear un gran número de direcciones IP, y es posible que se exceda el tiempo de espera antes de que finalice el escaneo. Utilice los campos Direcciones IP para definir un rango reducido de direcciones IP en el que espera encontrar clientes GIM en modalidad de escucha.
3. Pulse Descubrir para empezar a escanear clientes GIM en modalidad de escucha.
   Consejo: De forma predeterminada, el descubrimiento de clientes GIM y el despliegue de agentes de supervisión (S-TAP) se realiza en dos pasos separados: descubrimiento y luego despliegue. Esto le permite seleccionar manualmente los servidores de base de datos en los que desea instalar los S-TAP, tal como se describe en los pasos siguientes.

   Sin embargo, se puede racionalizar el proceso instalando automáticamente los S-TAP en todos los clientes GIM compatibles que se describen al escanear direcciones IP. Para habilitar la modalidad automática, pulse para abrir el diálogo Personalizar valores y seleccione Desplegar automáticamente agentes en servidores de base de datos descubiertos. Si utiliza la modalidad automática, después de especificar las direcciones IP que desea escanear, simplemente pulse el botón >Descubrir y desplegar.
4. En la sección Estado de servidor de base de datos, seleccione los servidores de base de datos en los que desea desplegar agentes de supervisión y pulse Desplegar agentes para abrir el diálogo Configurar agentes de supervisión.
5. En el diálogo Configurar agentes de supervisión, revise y ajuste los parámetros de instalación. Pule Desplegar para empezar a instalar agentes de supervisión.

   Los parámetros predeterminados deberían funcionar bien para la mayoría de los despliegues. Sin embargo, es posible que desee ajustar los siguientes valores para adaptarlos a su entorno.

   Directorio de instalación de Windows

   Especifique un directorio de instalación para los S-TAP desplegados en servidores de base de datos Windows. El parámetro se pasa por alto y se utilizan las vías de acceso de instalación predeterminadas cuando el despliegue se realiza en otras plataformas. Para obtener más información sobre los parámetros de instalación de S-TAP, consulte S-TAPs y otros agentes.

   Asignar un recopilador de Guardium

   Seleccione Utilizar el equilibrio de carga de empresa para asignar los S-TAP automáticamente en función de la carga relativa o de la disponibilidad de los recopiladores de Guardium en un entorno gestionado centralmente. Para obtener más información, consulte Equilibrio de carga empresarial.

   Seleccione Especificar recopilador para asignar los S-TAP a un recopilador de Guardium específico.
6. En la sección Estado de servidor de base de datos, utilice la columna Estado de instalación de S-TAP para supervisar el progreso de instalación de módulos. El instado `Instalado` indica que la instalación ha finalizado correctamente.

Qué hacer a continuación

Si el Estado de instalación de S-TAP de un servidor de base de datos está marcado como `Ha fallado`, pulse el icono para ver más información sobre el problema. Si un servidor de base de datos desaparece del Estado de servidor de base de datos después de intentar desplegar agentes de supervisión, pulse Registro de errores para obtener más información sobre el problema.

Consejo: El Registro de errores captura los problemas relacionados con la herramienta Desplegar agentes de supervisión. Por ejemplo, si Desplegar agentes de supervisión no encuentra un módulo necesario para la instalación, se añade un mensaje al Registro de errores. Otros errores se registran en registros específicos del componente y se pueden investigar pulsando el icono en la columna Estado de instalación de S-TAP.

Después de desplegar correctamente los agentes de supervisión, estará listo para supervisar el tráfico de los servidores de base de datos y para empezar a cumplir con los requisitos de cumplimiento de seguridad. Para configurar la supervisión del cumplimiento, vaya a Configuración > Inicio rápido > Supervisión del cumplimiento y consulte Inicio rápido para la supervisión del cumplimiento para obtener más información.

Tema principal: Inicio rápido para desplegar agentes de supervisión

Gestión de software con GIM

- Configuración por cliente
  Despliegue con rapidez S-TAP y otros paquetes de software mediante la herramienta Configuración por cliente de Guardium Installation Manager (GIM).
- Interfaces de usuario de GIM
  La finalidad de GIM es proporcionar capacidad de instalación automática para módulos, aprovechando el cliente GIM y el servidor GIM que residen en cada servidor de base de datos y sistema Guardium respectivamente.
- Interfaz de línea de mandatos de GIM
  Puede utilizar la CLI para instalar o actualizar módulos en el servidor de base de datos.

Tema principal: Guardium Installation Manager

Configuración por cliente

Despliegue con rapidez S-TAP y otros paquetes de software mediante la herramienta Configuración por cliente de Guardium Installation Manager (GIM).

Antes de empezar

Antes de utilizar la herramienta Configuración por cliente, verifique lo siguiente:

- Los clientes GIM están instalados en servidores de base de datos y conectados al sistema Guardium.
- Se han subido e importado lotes compatibles con GIM en el sistema Guardium.

Procedimiento

1. Vaya a Gestionar > Instalación de módulo > Configuración por cliente.
2. En la sección Elegir clientes, seleccione los servidores de base de datos donde desea instalar o actualizar el software mediante GIM. Seleccione clientes individuales utilizando los recuadros de selección de la tabla o utilice el menú Seleccionar grupo de clientes para seleccionar un grupo de clientes. Pulse Siguiente para continuar.
   Atención: Si añade nuevos clientes utilizando la herramienta Configuración por cliente, renueve el navegador para ver los nuevos clientes.
3. En la sección Elegir lote, utilice el menú Seleccionar un lote para identificar el software que desea instalar o actualizar. Pulse Siguiente para continuar. Después de seleccionar un lote de software, la columna Acción de lote seleccionada indica la acción que se realizará para cada cliente:

   Instalar
   : El lote seleccionado se instalará en el cliente. Esta acción indica una primera instalación del software en el cliente.

   Actualizar
   : El lote se actualizará en el cliente. Esta acción indica que hay una versión anterior del software instalada actualmente en el cliente.

   Actualizar parámetros
   : Los parámetros del lote se actualizarán en el cliente. Esta acción indica que el software seleccionado y el software instalado actualmente son de la misma versión.

   Degradar
   : El lote seleccionado se instalará en el cliente. Esta acción indica que el software seleccionado es más antiguo que el software actualmente instalado en el cliente.

   Ninguna (lote no encontrado)
   : No se llevará a cabo ninguna acción, lo que indica que no hay acciones compatibles en el cliente para el lote seleccionado.

   Ninguna (versión instalada más reciente)
   : No se realizará acción alguna porque el lote seleccionado es anterior a la versión que está actualmente instalada en el cliente. Para instalar una versión antigua del software, desinstale la versión instalada actualmente antes de instalar la versión deseada.

   Consejo:
   - Deseleccione el recuadro de selección Mostrar sólo últimas versiones para ver y trabajar con versiones anteriores de un lote.
   - Deseleccione el recuadro de selección Mostrar sólo lotes para identificar módulos individuales dentro de un lote.
   - Marque el recuadro de selección Mostrar sólo los clientes compatibles para ocultar los clientes que no sean compatibles con el lote seleccionado.

   Atención:
   - De forma predeterminada, el menú Seleccionar un lote muestra sólo la última versión del lote subido independientemente de la plataforma o la compatibilidad con los clientes seleccionados. Para instalar una versión de lote diferente para una plataforma específica o un cliente específico, desmarque el recuadro de selección Mostrar sólo las últimas versiones y seleccione el lote necesario.
   - Si sube e importa lotes nuevos mientras utiliza la herramienta Configuración por cliente, renueve el navegador para ver los nuevos lotes.
   - Si ya tenía un lote planificado para la instalación, la instalación de un nuevo lote eliminará la planificación existente.
4. En la sección Elegir parámetros, especifique valores para los parámetros obligatorios y opcionales. Utilice los iconos o para añadir o eliminar parámetros opcionales. Utilice el icono para buscar parámetros por nombre o por descripción. Pulse Siguiente para continuar.
   Importante: A menos que estén identificados como parámetros específicos del cliente, los valores proporcionados en la sección Elegir parámetros se aplican a todos los clientes en los que se instalará o actualizará el software. Para los parámetros específicos del cliente, el campo del valor está inhabilitado y los valores se definen por cliente en la sección Configurar clientes.
5. En la sección Configurar clientes, utilice la tabla para revisar y editar valores de parámetros para cada cliente. Los parámetros que se pueden editar muestran un icono junto al valor del parámetro. Pulse el icono para editar el valor.
6. Pulse Instalar para comenzar la instalación del software. Utilice el icono para planificar la instalación y luego pulse Aceptar para continuar.

Qué hacer a continuación

Utilice la sección Elegir lote para supervisar la instalación de software. El estado de la instalación se muestra en la columna Estado. Utilice el icono para renovar el estado de la instalación.
Tema principal: Gestión de software con GIM

Interfaces de usuario de GIM

La finalidad de GIM es proporcionar capacidad de instalación automática para módulos, aprovechando el cliente GIM y el servidor GIM que residen en cada servidor de base de datos y sistema Guardium respectivamente.

Los usuarios también interactúen con GIM a través de la CLI. Consulte Interfaz de línea de mandatos de GIM para obtener información sobre cómo instalar y actualizar módulos con GIM mediante la CLI.

Puede utilizar la GUI de Guardium Installation Manager (GIM) para realizar estas tareas:

- Supervisión de procesos
- Subir paquetes de módulos
- Configurar, instalar o actualizar módulos (por cliente)
- Configurar, instalar o actualizar módulos (por módulo)
- Mecanismo de retrotracción

Nota: Si se está utilizando A-TAP, primero debe inhabilitarse A-TAP en el servidor de base de datos antes de realizar una actualización o desinstalación de S-TAP basada en GIM.
Nota: GIM no da soporte a la instalación de instaladores de S-TAP nativos (rpm, dept, bff, etc.)
Nota: La instalación de módulos en un cliente específico por PRIMERA VEZ mediante el programa de utilidad GIM debe realizarse en formato de LOTE. Las futuras actualizaciones de módulos específicos que forman parte del lote instalado se pueden realizar como módulos individuales o como lotes.

Supervisión de procesos

Muestra el estado de los procesos de GIM en los servidores.

Supervisor

El supervisor de GIM es un proceso cuyo principal objetivo es supervisar los procesos de Guardium. En concreto, es el responsable de iniciar, detener y garantizar que todos los procesos de Guardium se están ejecutando en todo momento y de reiniciarlos si fallan.

Nota: Para Guardium V9.0, en Solaris 5.10/5.11, GIM y SUPERVISOR ahora son servicios SMF. Ya no son entradas de inittab.

Para iniciar/detener gim/supervisor utilice:

svcadm -v enable guard_gim

svcadm -v enable guard_gsvr

svcadm -v disable guard_gim

svcadm -v disable guard_gsvr

GIM

El proceso GIM es el proceso del cliente GIM, que es el responsable de tareas como registrarse ante el servidor GIM, iniciar una solicitud para comprobar si hay actualizaciones de software, instalar el nuevo software, actualizar parámetros de módulos y desinstalar módulos.

Subir paquetes de módulos

Carga el archivo de paquetes de módulos (un archivo .gim que contiene los subpaquetes del módulo o módulos) en la base de datos.

1. Pulse Gestionar > Gestión de instalación > Subirpara abrir la ventana Subir.
2. Pulse Examinar para ver dónde se encuentra el paquete (archivo .gim) en el disco.
3. Pulse Subir para subir el paquete.
4. Pulse el icono Importar del paquete subido situado bajo Importar módulos subidos para subir el paquete.

Configurar, instalar o actualizar módulos (por cliente)

Consejo: Para obtener información sobre las últimas herramientas de gestión de software, consulte Configuración por cliente.

Puede utilizar esta opción para configurar/instalar un módulo para tantos clientes como desee desde paquetes ya cargados.

La forma más sencilla, segura y rápida de instalar o desinstalar módulos es mediante el uso de lotes. La utilización de lotes garantiza la dependencia automática y la resolución de clasificaciones.

Si ya ha creado grupos de clientes, puede utilizar un grupo para especificar los clientes como destino de la acción especificada. De lo contrario, siga estos pasos para seleccionar una lista de clientes.

1. Pulse Gestionar > Gestión de instalación > Configurado por cliente(Antiguo) para abrir los Criterios de búsqueda de cliente.
2. Pulse el botón Buscar para realizar una búsqueda filtrada y visualizar el panel Clientes.
3. Seleccione los clientes que constituirán el destino de la acción especificada.
   - Si hay más de 20 clientes, la lista de clientes se divide en páginas adicionales.
     Nota: Si se pulsa el botón Seleccionar todo, solo se seleccionarán los clientes de la página actual que se está visualizando
4. En el panel Clientes se pueden realizar dos acciones:
   - Configurar/instalar parámetros comunes
   - Configurar/instalar un módulo
   - Restablecer clientes: si se pulsa Restablecer clientes, se pueden disociar módulos de los clientes seleccionados y eliminar la definición de cliente de la base de datos del sistema Guardium. Nota: cuando se restablece un cliente NO se activa la eliminación del módulo en el servidor de base de datos.
   - Ver estado de instalación de este cliente: si pulsa el icono de información, puede abrir el panel Estado de instalación y ver el estado de instalación de un cliente. Este panel muestra todos los módulos del cliente que se han instalado o para los que se ha planificado una actualización o desinstalación. Desde este panel, puede utilizar el icono Editar este módulo para configurar parámetros para cada módulo de forma individual.

Configurar, instalar o actualizar módulos (por módulo)

Empezando por los módulos, permite a los usuarios configurar e instalar un módulo para tantos clientes como desee. Los paquetes necesarios se deben haber cargado de antemano.

1. Pulse Gestionar > Instalación de módulo > Configuración por módulo para abrir los Criterios de búsqueda de módulos.
2. Pulse Buscar para realizar una búsqueda filtrada y visualizar el panel Módulos que muestra todos los módulos y lotes disponibles.
3. Seleccione uno o varios módulos y pulse Siguiente para abrir el panel Clientes.
4. Seleccione los clientes que constituyen el destino de la acción especificada.
   Nota: Si hay más de 20 clientes, la lista de clientes se divide en páginas adicionales. Si se pulsa el botón Seleccionar todo, solo se seleccionan los clientes de la página actual que se está visualizando
5. En el panel Clientes se pueden realizar estas acciones:
   - Instalar/actualizar módulos: seleccione uno o varios clientes de destino y pulse Siguiente; luego pulse Instalar/Actualizar
   - Modificar la configuración de parámetros de módulos: seleccione uno o varios clientes de destino y pulse Siguiente, modifique los valores de los parámetros, seleccione los clientes de destino y pulse Aplicar a clientes
   - Pulse Restablecer clientes para disociar módulos de los clientes seleccionados y eliminar la definición de cliente de la base de datos del sistema Guardium. Nota: cuando se restablece un cliente NO se activa la eliminación del módulo en el servidor de base de datos.
   - Puede ver el estado de instalación de este cliente si pulsa el icono de información para abrir el panel Estado de instalación y ver el estado de la instalación de un cliente. Este panel muestra todos los módulos del cliente que se han instalado o para los que se ha planificado una actualización. Desde este panel, se puede utilizar el icono Editar este módulo para configurar parámetros para cada módulo de forma individual.
   - Pulse Ejecutar diagnósticos: el informe de diagnósticos se ejecuta la próxima vez que los clientes envían un mensaje de actividad y se registran en la Lista de sucesos de GIM.

Configurar/instalar parámetros comunes

1. Pulse Configuración > Herramientas y vistas > Configuración de parámetros.
2. Seleccione los clientes de la sección Parámetros de módulos de cliente cuyos parámetros desea modificar
3. Modifique cualquiera de los parámetros de módulo que aparecen en la lista de la sección Parámetros de módulo de cliente
   Nota: los parámetros se pueden especificar en la sección Parámetro de módulo común pulsando Aplicar a seleccionados para llenar los clientes seleccionados en la sección Parámetros de módulo de cliente.
4. Pulse Aplicar a clientes, después de especificar valores para todos los parámetros necesarios en todos los clientes seleccionados, para guardar la configuración en la base de datos. Antes de guardar, se realiza una validación para garantizar que todos los campos necesarios tienen valores o que sus valores están en un rango predefinido.
5. Después de guardar las configuraciones, pulse Instalar/Actualizar para planificar la instalación del módulo en los clientes seleccionados. Además, desde el panel Parámetros del módulo puede desinstalar, cancelar la instalación/actualización, cancelar la desinstalación y revertir los cambios actuales. Tenga en cuenta que la fecha y hora de la planificación corresponden a la fecha y hora de los clientes seleccionados.
   Nota: El botón Generar Grdapi de la parte delantera de la línea de cliente bajo la sección Parámetro de módulo de cliente le permite ver la lista de mandatos grdapi que reflejan los cambios que ha realizado en el módulo como, por ejemplo, asignación, desinstalación, planificación y actualización del módulo. Estos mandatos grdapi se proporcionan para que pueda tomar el conjunto de mandatos y aplicarlos a otros clientes en un script si desea reproducir los cambios.
   Nota: El botón Abrir contenido de propiedad aparece delante de cada propiedad que se puede escribir y abre una ventana que facilita la edición de un campo largo.
   Nota: El botón Ver estado de instalación de este cliente, que también está delante de la línea de cliente bajo la sección Parámetro de módulo de cliente, proporciona una vista del estado actual de la instalación del módulo.
   Nota: Cuando se instala KTAP como parte de BUNDLE-STAP, el estado de KTAP se establecerá en INSTALLED aunque falte el módulo KTAP real para esta plataforma específica. Sin embargo, se mostrará un mensaje en el informe GIM-EVENTS que indicará que falta el módulo KTAP.
   Nota: Debe comprobar el informe GIM-EVENTS después de instalar lotes en los servidores de BD.
6. Pulse Atrás para volver al panel Clientes.

Parámetros de S-TAP de Windows en GIM

El parámetro WINSTAP_CMD_LINE se puede utilizar para especificar opciones de instalación adicionales, como por ejemplo el control de la instalación de determinadas características (DB2, Oracle, CAS, etc).

Si no se especifica nada además de la línea de mandatos predeterminada. las características se instalan de acuerdo con el conjunto de características de una instalación típica.

Esta es la lista de opciones, que se pueden establecer en 0 (no instalado) o en 1 (instalado).

- MSSQLSharedMemory
- DB2SharedMemory
- CAS
- NamedPipes
- START: este parámetro controla si S-TAP se inicia o no después de la instalación.
- INSTALL_DIR: este parámetro especifica dónde se debe instalar el software.
- QUIET: controla los conmutadores que se pasan al instalador de Windows utilizado para depurar problemas de instalación; no realice ningún cambio.
- DBALIAS: un alias de la máquina del servidor de base de datos que puede utilizar el nombre de host de la máquina y no está relacionado con la base de datos real instalada en el servidor.
- AUTO_DISCOVERY

  Se utiliza para el descubrimiento automático de bases de datos en el sistema y la creación de los motores de inspección. 0=desactivado, 1=activado, el valor predeterminado es 1. Utilice 0 para inhabilitar el descubrimiento automático.

Por ejemplo, las siguientes opciones de línea de mandatos:

```
CAS=0 NamedPipes=0
```

Omitirán la instalación de soporte de CAS y de conductos con nombre.
Si está instalando un S-TAP y no desea que descubra automáticamente las bases de datos de MSSQL, escriba `START=0` en la columna WINSTAP_CMD_LINE para impedir que el S-TAP se inicie cuando se instala. También puede especificar este parámetro para un servidor de bases de datos individual utilizando la API de GIM:

```
grdapi gim_update_client_params clientIP=xx.xx.xx.xx paramName=WINSTAP_CMD_LINE paramValue="START=0"
```

El directorio de instalación para el S-TAP debe estar vacío o no existir. No puede instalar un S-TAP en un directorio que ya contenga archivos. En el caso de instalaciones en máquinas de 64 bits, debe especificar la carpeta de archivos de programa de 32 bits (por ejemplo, C:/program files (x86)/guardium/stap, NO C:/program files/guardium/stap). De lo contrario, la instalación fallará porque no se podrá escribir en las carpetas de 64 bits.

Durante la instalación también se pueden definir parámetros guard_tap.ini adicionales. Un ejemplo es paramValue="START=1 !client_timeout_sec=120&use_tls=1!"

Nota: cuando se utilizan mandatos de GuardAPI, el valor del parámetro WINSTAP_CMD_LINE debe ir entre comillas y cada parámetro separado por espacios, como sucede en paramValue="START = 1 CAS= 0 " en el ejemplo anterior. Si faltan de espacios es posible que la instalación subsiguiente no se complete como se esperaba.

Configurar/instalar un módulo

1. Si está configurando, instalando o actualizando:
   a. por cliente
      i. Pulse Siguiente para visualizar el panel Módulos comunes, donde se puede instalar una lista de todos los lotes y módulos comunes disponibles en los clientes seleccionados.
      ii. Seleccione el módulo o lote que desea configurar o instalar para los clientes seleccionados.
      Nota: El estado de un módulo o lote solo se muestra si su versión coincide con una versión instalada o con una versión planificada.
      iii. Pulse Siguiente después de seleccionar un módulo o lote de la lista.
   b. por módulo
      i. Pulse Siguiente después de seleccionar los clientes de la lista
2. Dependiendo del módulo o lote seleccionado, y de las posibles dependencias, verá opciones basadas en los tipos de selección:
   - Lote
     Si pulsa Siguiente para un lote, irá al panel Parámetros de módulo que mostrará todos los parámetros correspondientes a todos los módulos del lote.
     Modifique cualquiera de los parámetros de módulo que aparecen en la lista de la sección Parámetros de módulo de cliente.
     Nota: Un lote se trata como un módulo normal.
   - módulo sin dependencias obligatorias

Si pulsa Siguiente para módulos sin dependencias obligatorias, irá al panel Parámetros de módulo que mostrará los parámetros del módulo. Modifique cualquiera de los parámetros de módulo que aparecen en la lista de la sección Parámetros de módulo de cliente.

- módulo con dependencias
  Si pulsa Siguiente para un módulo con dependencias, se visualizará dicho módulo y todos los módulos de dependencias en la pantalla Módulos dependientes. Pulse el icono Editar de cualquiera de los módulos para configurar sus parámetros para todos los clientes seleccionados, lo que le llevará al panel Parámetros de módulo, que mostrará los parámetros del módulo. Cambie los parámetros que desee y pulse el botón Aceptar para volver a la pantalla Módulos dependientes.
  Nota: La configuración del módulo y de todas sus dependencias se puede guardar en la base de datos una sola vez. Además solo se pueden instalar como un lote. Esto significa que no se pueden guardar ni se puede planificar su instalación de forma individual. Si, por ejemplo, en medio de una instalación de planificación el proceso falla para uno de los módulos en uno de los clientes, se retrotraerán todas las instalaciones anteriores a ese error.
  Nota: los parámetros se pueden especificar en la sección Parámetro de módulo común pulsando Aplicar a seleccionados para llenar los clientes seleccionados en la sección Parámetros de módulo de cliente.

3. Pulse Aplicar a clientes, después de especificar valores para todos los parámetros necesarios en todos los clientes seleccionados, para guardar la configuración en la base de datos. Antes de guardar, se realiza una validación para garantizar que todos los campos necesarios tienen valores o que sus valores están en un rango predefinido.
4. Después de guardar las configuraciones, pulse Instalar/Actualizar para planificar la instalación del módulo y sus dependencias en los clientes seleccionados. Además, desde el panel Parámetros de módulo dependiente puede desinstalar, cancelar la instalación/actualización, cancelar la desinstalación y revertir los cambios actuales. Tenga en cuenta que la fecha y hora de la planificación corresponden a la fecha y hora de los clientes seleccionados.
   Nota: El botón Generar Grdapi que hay delante de la línea de cliente bajo la sección Parámetro de módulo de cliente permite al usuario ver la lista de mandatos grdapi que reflejan los cambios que el usuario ha realizado en el módulo como, por ejemplo, la asignación, la desinstalación, la planificación y la actualización del módulo. Estos mandatos grdapi se proporcionan al usuario para que pueda tomar el conjunto de mandatos y aplicarlos a otros clientes en un script si desea reproducirlos.
   Nota: El botón Abrir contenido de propiedad aparece delante de cada propiedad que se puede escribir y abre una ventana que facilita la edición de un campo largo.
   Nota: El botón Ver estado de instalación de este cliente, que también está delante de la línea de cliente bajo la sección Parámetro de módulo de cliente, proporciona una vista del estado actual de la instalación del módulo.
   Nota: Cuando se instala K-TAP como parte de BUNDLE-STAP, el estado de K-TAP se establece en INSTALLED aunque falte el módulo K-TAP real para esta plataforma específica. Sin embargo, se mostrará un mensaje en el informe GIM-EVENTS que indicará que falta el módulo K-TAP.
   Nota: Compruebe siempre el informe GIM-EVENTS después de instalar lotes en los servidores de BD.
   Nota: Cuando se desinstalan módulos, GIM solo desinstala el módulo seleccionado, no las dependencias.

Mecanismo de retrotracción

La finalidad del mecanismo de retrotracción de GIM es manejar los errores durante la instalación y recuperar los módulos a su estado anterior. El mecanismo de retrotracción da soporte a los siguientes escenarios de recuperación:

1. Recuperación de actualización dinámica
   Para lotes
   - Cuando se instalan lotes, la recuperación retrotraer los módulos que tienen un error de instalación dentro del lote.
   - Los módulos que están marcados como `NO_ROLLBACK` (en forma del parámetro de solo lectura <MODULE>_NO_ROLLBACK=1) no se retrotraerá en el caso de que se produzca un error. S-TAP/KTAP son dos de estos módulos que, una vez instalados correctamente, no se retrotraerán en el caso de que se produzca un error en otro módulo.

   Para no lotes
   - La retrotracción implica eliminar el módulo autónomo en el caso de una instalación desde cero o revertir a la versión anterior en el caso de una actualización.
2. Recuperación de la instalación en el momento de arrancar
   Si se produce un error de instalación durante un rearranque del sistema, se necesitará un segundo reinicio del sistema para poder completar la recuperación. Los usuarios seguirán viendo el estado IP-PR después del rearranque y una entrada GIM_EVENT que indicará que es necesario un segundo rearranque para completar el proceso de recuperación. Luego el estado del módulo/lote indicará el estado "FAILED" después del segundo rearranque.
   Nota: Si el estado es 'IP-PR', el arranque del servidor de BD varía en función del sistema operativo (cualquier otra forma de rearrancar el sistema mantiene los módulos pendientes en estado pendiente):

   ```
   Linux   : shutdown -r
   SuSe    : reboot
   HP      : shutdown -r
   Solaris : shutdown -i [6|0]  (Nota : '0' solo se puede utilizar si el cierre se realiza desde un servidor de terminal)
   AIX     : reboot
   Tru64   : reboot
   ```

   Nota: Además, antes de volver a arrancar, las instancias de A-TAP se deben inhabilitar o desactivar.

Cambio del servidor GIM para un cliente GIM

Puede cambiar el servidor GIM que gestiona uno o varios clientes GIM. Es posible que desee realizar este cambio para equilibrar la carga entre los servidores GIM o para facilitar la distribución de paquetes de GIM. Para volver a asignar un grupo de clientes GIM a un servidor GIM diferente, siga estos pasos:

1. Pulse Gestionar > Gestión de instalación > Configurar por módulo para cambiar el servidor GIM correspondiente a un cliente GIM.
2. Seleccione un lote de GIM que esté instalado en los clientes que desea reasignar. Pulse Siguiente.
3. Seleccione los clientes que desea cambiar. Puede pulsar Seleccionar todo o puede seleccionar clientes individualmente. Pulse Siguiente.
4. Pulse Seleccionar todo.
5. Para el parámetro GIM_URL, especifique el nombre de host o la dirección IP del servidor GIM (sistema Guardium) al que desea reasignar los clientes GIM seleccionados. Pulse Aplicar a seleccionados.
6. En el mismo panel, pulse Aplicar a clientes y, a continuación, pulse Instalar/Actualizar y planifique la actualización.

Una vez procesada la actualización, el nuevo servidor GIM gestionará el cliente GIM.
Tema principal: Gestión de software con GIM

Interfaz de línea de mandatos de GIM

Puede utilizar la CLI para instalar o actualizar módulos en el servidor de base de datos.

En los siguientes ejemplos solo se cubren algunos de los escenarios más comunes. Para obtener más información y para ver una lista completa de todos los mandatos de CLI soportados, consulte las funciones GIM de GuardAPI.

- Carga de paquetes de módulos
- Actualización o instalación desde cero mediante lotes
- Desinstalación de un módulo o lote
- Estado de la instalación
- Consulta del estado de módulos

Carga de paquetes de módulos

Para que los módulos se puedan instalar en el servidor de BD, se deben cargar en la base de datos GIM del gestor central. Si un gestor central no forma parte de la arquitectura, los paquetes se deben cargar en cada sistema Guardium. Utilice la opción Cargar paquete de la IU de GIM para que los paquetes se carguen en la base de datos.

Actualización o instalación desde cero mediante lotes

Nota: La instalación desde cero también se refiere a los casos en que se instala un S-TAP antiguo (previo a GIM) en el servidor de base de datos.
Un lote es una lista de módulos agrupados para facilitar el proceso de instalación. Utilice siempre lotes para instalar o actualizar módulos.

1. Obtenga una lista de clientes registrados (es decir, servidores de base de datos instalados con el cliente GIM que se han registrado con el servidor GIM):

```
grdapi gim_list_registered_clients
ID=0
####### ENTRY 0 #######
CLIENT_ID:          1
IP:                 192.168.2.204
OS:                 HP-UX
OS_RELEASE:         B.11.00
OS_VENDOR:          hp
OS_VENDOR_VERSION:  B.11.00
OS_BITS:            64
PROCESSOR           9000
####### ENTRY 1 #######
CLIENT_ID:          2
IP:                 192.168.2.210
OS:                 Linux
OS_RELEASE:         2.6.16.54-0.2.5-smp
OS_VENDOR:          suse
OS_VENDOR_VERSION:  10.1
OS_BITS:            64
PROCESSOR           x86_64
```

2. Asigne (es decir, prepare para instalar; NO es una solicitud para instalarlo realmente en el cliente) el último lote disponible para un cliente específico

```
grdapi gim_assign_latest_bundle_or_module_to_client  clientIP=198.168.2.210 moduleName=BUNDLE-STAP
```

   Nota: Para asignar un lote o módulo específico a un cliente, el paso 2 se debe sustituir por la siguiente secuencia:

```
gim_get_available_modules clientIP=”client ip”
gim_assign_bundle_or_module_to_client_by_version clientIP=”client ip” modulesName=”Bundle/Module name”
moduleVersion=”Bundle/Module version”
```

3. Planifique la instalación.

```
grdapi gim_schedule_install clientIP=192.168.2.210 date=now
```

   Nota: Para instalaciones de varios clientes, repita los pasos 2-3.
   Nota: Para una planificación flexible de GIM, utilice now + [1-9][0-9]* minute | hour | day | week | month. Ejemplo: now + 1 day, now + 3 minutes

Planificación de GIM

Cualquier hora es relativa a la hora del sistema Guardium. Now significa ahora mismo, tal como esté especificado en el sistema Guardium. Now +30 minute es la hora del sistema Guardium + 30 minutos. Lo verá si mira el estado de la instalación pulsando en la pequeña "i" que hay junto al cliente, por ejemplo en Gestionar > Instalación de módulo > Configurado por el cliente (Antiguo). Si la hora del servidor de base de datos ha pasado la hora del sistema Guardium especificada para la instalación, comienza la instalación.

Ejemplo uno: configure tres clientes (a) definido para la hora del sistema - 1 hora, (b) definido para la hora del sistema Guardium y (c) definido para la hora del sistema Guardium + 1 hora.

Configure una instalación de S-TAP mediante GIM para "now +30 minute".

El sistema Guardium (a), que ya está 30 minutos adelantado con relación a la hora establecida para la instalación, se instalará de inmediato.

El sistema Guardium (b) se instalará en 30 minutos.

El sistema Guardium (c) se instalará una hora después que (b).

Ejemplo dos - Misma configuración como ejemplo, pero ahora especifique "now".

El estado de la instalación cambia por IP inmediatamente en todos los clientes.

Desinstalación de un módulo o lote

```
grdapi gim_uninstall_module clientIP=192.168.2.210 module=BUNDLE-STAP date=now
```

Puede especificar `date=now` o utilizar el formato `AAAA-MM-DD HH:mm`. La desinstalación tendrá lugar la próxima vez que el cliente GIM compruebe si hay actualizaciones (GIM_INTERVAL).

Estado de la instalación

Se puede recuperar información adicional sobre el último estado que ha enviado el cliente ejecutando el siguiente mandato (el mensaje de estado aparecerá como entrada en la tabla GIM_EVENTS desde la que se puede generar un informe):

Puede obtener el mensaje de estado general ejecutando el siguiente mandato de la CLI:

```
grdapi gim_get_client_last_event clientIP="client ip"
grdapi gim_get_client_last_event clientIP=winx64
grdapi gim_get_client_last_event clientIP=9.70.144.73
```

Aquí se muestra un ejemplo de la información que genera este mandato:

```
ID=0
OK
BUNDLE-STAP-8.0_r2609_1 INSTALLED
STAP-UTILS-8.0_r2609_1 INSTALLED
COMPONENTS-8.0_r2609_1 INSTALLED
KTAP-8.0_r2609_1 INSTALLED
STAP-8.0_r2609_1 INSTALLED
TEE-8.0_r2609_1 INSTALLED
ATAP-8.0_r2609_1 INSTALLED
```

Consulta del estado de módulos

Para consultar el estado del módulo instalado por cliente, hay que ejecutar el siguiente mandato de la CLI.

```
grdapi gim_list_client_modules clientIP=”client ip”
```

Se pueden mostrar los siguientes estados:

INSTALLED
: El módulo está instalado.

PENDING-INSTALL
: El módulo está pendiente de que se planifique su instalación.

PENDING-UNINSTALL
: El módulo está pendiente de que se planifique su desinstalación.

PENDING-UPDATE
: El módulo está pendiente de que se planifique su actualización.

IP
: Se está procesando la instalación del módulo.

FAILED
: La última operación del módulo ha fallado.

IP-PR
: El cliente tiene que rearrancar el módulo para completar el proceso de instalación. Antes de rearrancar, desactive todas las instancias de A-TAP. El rearranque del servidor de base de datos varía en función del sistema operativo. Cualquier otra forma de rearrancar el sistema dejará los módulos pendientes en estado pendiente.

  - AIX: reboot
  - Linux : shutdown -r
  - SuSe: reboot
  - HP-UX: shutdown -r
  - Solaris: shutdown -i [6|0] (Nota : '0' solo se puede utilizar si el mandato shutdown se ejecuta desde el servidor de terminal)
  - Tru64: reboot

Salida de ejemplo

```
ID=0
####### ENTRY 0 #######
MODULE_ID:          11
NAME:               INIT
INSTALLED_VERSION   8.0_r3852_1
SCHEDULED_VERSION   8.0_r3852_1
STATE:              INSTALLED
IS_SCHEDULED:       N
####### ENTRY 1 #######
MODULE_ID:          -1
NAME:               COMMON
INSTALLED_VERSION   8.0_r0_1
SCHEDULED_VERSION   8.0_r0_1
STATE:              INSTALLED
IS_SCHEDULED:       N
####### ENTRY 2 #######
MODULE_ID:          12
NAME:               UTILS
INSTALLED_VERSION   8.0_r3852_1
SCHEDULED_VERSION   8.0_r3852_1
STATE:              INSTALLED
IS_SCHEDULED:       N
####### ENTRY 3 #######
MODULE_ID:          13
NAME:               SUPERVISOR
INSTALLED_VERSION   8.0_r3852_1
SCHEDULED_VERSION   8.0_r3852_1
STATE:              INSTALLED
IS_SCHEDULED:       N
####### ENTRY 4 #######
MODULE_ID:          14
NAME:               GIM
INSTALLED_VERSION   8.0_r3852_1
SCHEDULED_VERSION   8.0_r3852_1
```

```
STATE:              INSTALLED
IS_SCHEDULED:       N
####### ENTRY 5 #######
MODULE_ID:          15
NAME:               BUNDLE-GIM
INSTALLED_VERSION   8.0_r3852_1
SCHEDULED_VERSION   8.0_r3852_1
STATE:              INSTALLED
IS_SCHEDULED:       N
```

Habilitación de K-TAP

Si, durante el proceso de instalación, K-TAP no se carga correctamente, posiblemente debido a una incompatibilidad de hardware o software, se instala Tee como mecanismo predeterminado de recopilación. Para volver a K-TAP, siga estos pasos una vez resueltos los problemas de compatibilidad.

1. Inhabilite S-TAP. Consulte Detener S-TAP de UNIX para obtener más información.
2. Edite guard_tap.ini y cambie *ktap_installed* por 1 y *tee_installed* por 0
3. Ejecute el mandato guard_ktap_loader install.

   ```
   ejemplo: /usr/local/guardium/guard_stap/ktap/current/guard_ktap_loader install
   ```

4. Ejecute el mandato guard_ktap_loader start.

   ```
   ejemplo: /usr/local/guardium/guard_stap/ktap/current/guard_ktap_loader start
   ```

5. Vuelva a habilitar S-TAP. Consulte Reiniciar S-TAP de UNIX para obtener más información.

Tema principal: Gestión de software con GIM

Asignación de servidores GIM

Se puede conectar de forma remota a un agente GIM preinstalado e inactivo (no conectado a ningún recopilador) y hacer que se conecte a algún recopilador sin necesidad de acceder al servidor de base de datos.

Visión general

El siguiente proceso (también denominado descubrimiento automático de GIM) le permite conectarse de forma remota a un agente GIM preinstalado e inactivo y hacer que se conecte a un recopilador sin acceder al servidor de base de datos.

1. Un cliente GIM inactivo se ejecuta en modalidad de escucha y espera una conexión de un recopilador.
2. Desde la interfaz gráfica de usuario (GUI) del recopilador o GuardAPI, puede enviar la dirección IP de cualquier recopilador al cliente GIM inactivo.
3. El cliente GIM inactivo acepta la dirección IP del recopilador y se conecta al mismo.

Si GIM se instala sin especificar la dirección IP de un recopilador (--sqlguardip), se ejecutará en modalidad de servidor. Cuando el agente GIM se ejecuta en modalidad de servidor, solo acepta mensajes de recopiladores verificados sobre SSL que tienen autenticación de certificado y verificación de secreto compartido. Si se producen 30 errores de autenticación consecutivos o más, el agente de GIM deja de estar a la escucha de solicitudes y se ejecuta en modalidad de servidor. Esta acción impide ataques de denegación de servicio (DoS).

Puede definir sus propios certificados, secreto compartido y número de puerto. Para utilizar otros certificados, especifique el nombre completo de vía de acceso del certificado o clave en los parámetros de instalación: --key_file y --cert_file. Cargue los certificados en el almacén de claves del recopilador con el mandato de GuardAPI store gim.

Para establecer un secreto compartido distinto del predeterminado, utilice el mandato de GuardAPI grdapi gim_set_global_param paramName=gim_listener_default_shared_secret paramValue=<password>. El formato debe ser una serie. El secreto compartido debe ser idéntico en el recopilador y en el servidor de base de datos.

Nota: No especifique el secreto compartido sin cifrar en la línea de mandatos.

Para utilizar un puerto que no sea el puerto predeterminado, especifique el puerto en el parámetro de instalación --listener_port. Establezca el parámetro global gim_listener_default_port de GIM con el nuevo puerto en los parámetros globales de GIM.

Nota: El puerto predeterminado o definido por el usuario debe estar habilitado en el cortafuegos.

Parámetros

En la lista siguiente se describen los parámetros de instalación de GIM:

- --sqlguardip - Establece la dirección IP/nombre de host al que se conecta el cliente GIM. Si no se especifica, el cliente GIM trabajará en "Modalidad de escucha".
- --ca_file - Vía de acceso y nombre completo del archivo PEM de la autoridad emisora de certificados.
- --key_file - Vía de acceso y nombre completo del archivo PEM de clave privada.
- --cert_file - Vía de acceso y nombre completo del archivo PEM de certificado.
- --shared_secret - Especifique un secreto compartido para verificar los recopiladores.
- --listener_port - Especifique un número de puerto distinto del predeterminado.
- --no_listener - Inhabilita la ejecución de GIM en "Modalidad de escucha", aunque no se especifique --sqlguardip.

Cualquier intento de:

- actualizar parámetros
- instalar módulos
- desinstalar GIM directamente en el servidor de base de datos

hace que el agente de GIM salga de la modalidad de servidor y procese la solicitud. Si el cliente GIM no puede conectarse al recopilador designado, vuelve a la modalidad de servidor. Después de asignar el agente de GIM a una dirección IP o un nombre de host de un recopilador válido, no puede establecer el servidor GIM de modo que se ejecute de nuevo en modalidad de servidor. Todos los nuevos parámetros de modalidad de servidor del agente GIM aparecen como de solo lectura (READ-ONLY).
Nota: Los parámetros siguientes deben existir en el sistema de archivos o la instalación falla:

- ca_file
- key_file
- cert_file

Parámetro adicional de línea de mandatos

GIM y los instaladores consolidados para GIM tienen un parámetro de línea de mandatos adicional:

--allow_ip_hostname_combo <0|1>

nombre de parámetro : GIM_ALLOW_IP_HOST_COMBO

valores del parámetro: 1 - Habilitado, 0 - Inhabilitado

Valor predeterminado del parámetro : 0

descripción del parámetro : Si está habilitado y GIM_CLIENT_IP es distinto del nombre de host del servidor de bd, GIM_CLIENTS.GIM_CLIENT_NAME se establecerá con un valor que es la combinación de `hostname`_<GIM_CLIENT_IP>.

Si GIM_CLIENT_IP está establecido con una dirección IP y GIM_ALLOW_IP_HOST_COMBO está habilitado, el nombre de host de GIM será una combinación de <hostname>_<GIM_CLIENT_IP> Esto permitirá la exclusividad de los clientes GIM entre los servidores de base de datos con un nombre de host "común".

LIMITACIÓN: NO puede establecer GIM_CLIENT_IP con un nombre de host "común". Esto se considerará un intento de registrarse con un identificador duplicado.

Definición de GIM en los parámetros globales en modalidad de servidor

Puede configurar los parámetros de GIM en modalidad de servidor con el siguiente mandato GuardAPI:

```
grdapi gim_set_global_param
paramName=gim_listener_default_shared_secret
paramValue=<password>
```

Este valor se cifra y se almacena en la base de datos. El valor debe ser idéntico al valor no cifrado como secreto compartido si instala el agente GIM en el servidor de base de datos.

Para configurar un nuevo puerto de GIM predeterminado en modalidad de servidor, utilice el siguiente mandato de GuardAPI:

```
grdapi gim_set_global_param paramName=gim_listener_default_port paramValue=<número puerto>
```

Este valor debe ser idéntico al valor no cifrado del secreto compartido si instala el agente GIM en el servidor de base de datos.

Nota: Si utiliza otro puerto o secreto compartido, debe especificar el puerto o secreto compartido cada vez que conecte el IP o nombre de host del recopilador al agente de GIM en modalidad de servidor.

Activación remota de GIM

Puede conectarse de forma remota a un agente GIM preinstalado y conectarlo a un recopilador sin acceder al servidor de base de datos con la activación remota de GIM.

1. Pulse Gestionar > Instalación de módulo > Activación remota de GIM.
2. Escriba la dirección IP o el nombre de host en el que se ejecuta GIM en modalidad de escucha en el campo IP / nombre de host. También puede seleccionar un grupo de servidores en la siguiente lista.
3. Escriba un valor numérico en Puerto de escucha GIM si no coincide con el valor global de GIM. El valor predeterminado es 8445.
4. Especifique el secreto compartido en el campo Contraseña de escucha GIM si es distinto del valor global de GIM.
5. Pulse Enviar para procesar la información o Restablecer para borrar la información.

Nota: Debe especificar una dirección IP o un nombre de host o seleccionar un grupo de servidores, pero el puerto de escucha GIM y la contraseña de escucha GIM son opcionales. Cuando instala el cliente GIM en modalidad de escucha, los valores del secreto compartido y de los certificados no se pueden cambiar a menos que vuelva a instalar el cliente GIM.
Nota: Si el campo "IP de recopilador" de la activación remota de GIM está en blanco, el nombre de host del recopilador se envía al servidor. Si se especifica una IP, se envía esta en su lugar.

Creación de un proceso de descubrimiento automático de GIM

Especifique el host y los puertos que escanea el proceso de descubrimiento automático.

1. Para configurar el descubrimiento automático, pulse Descubrir > Descubrimiento de base de datos > Configuración de descubrimiento automático de GIM.
2. Pulse Nuevo para crear un proceso nuevo y abrir el Creador de proceso de descubrimiento automático.
3. Especifique un Nombre de proceso que sea exclusivo en el sistema Guardium.
4. Para ejecutar un trabajo de sondeo inmediatamente después de que se complete el trabajo de escaneo, marque el recuadro de selección Ejecutar sondeo después de escaneo.
5. Para cada host o subred que se vaya a escanear, especifique el host y el puerto y pulse Añadir escaneo. Cada vez que añade un escaneo, este se añade a la lista de tareas.
   Nota:
   - Los caracteres comodín están habilitados. Por ejemplo: para seleccionar todas las direcciones que empiezan por 192.168.2, utilice 192.168.2.*.
   - Especifique un rango de puertos colocando un guión entre el primer número de puerto y el último del rango. Por ejemplo: 4100-4102.
   - Después de añadir un escaneo, modifique el host o el puerto escribiendo sobre el mismo. Pulse Aplicar para guardar la modificación.
   - Si tiene una configuración de pila dual, tendrá que configurar un escaneo para las direcciones IPV4 y para las direcciones IPV6.
   - Para eliminar un escaneo, pulse el icono Suprimir esta tarea correspondiente al escaneo. Si una tarea tiene resultados de escaneo dependientes, el escaneo no se puede suprimir.
6. Cuando haya terminado de añadir escaneos, pulse Aplicar y ejecute el trabajo o planifique el trabajo para su futura ejecución. Consulte Planificación si necesita definir una planificación.

Parámetros globales de GIM

Defina su propio secreto compartido o puerto de escucha GIM a través de la interfaz de usuario.

1. Para abrir los Parámetros globales de GIM, pulse Gestionar > Instalación de módulo > Parámetros globales de GIM.
2. Seleccione gim_listener_default_shared_secret para definir el secreto compartido o gim_listener_default_port para definir el puerto.
3. Pulse el icono para editar el parámetro seleccionado.
4. Cambie el valor y pulse Guardar para cambiar el parámetro o Cerrar para volver a la página.

Tema principal: Guardium Installation Manager

Instalación del cliente GIM en un servidor Windows

Obtenga información sobre cómo instalar el cliente GIM para Windows mediante un instalador interactivo o una instalación silenciosa. También encontrará instrucciones para desinstalar el cliente GIM.

Acerca de esta tarea

Actualmente existen dos tipos de instaladores para el cliente GIM en función de la versión del cliente GIM. La versión 10.1.2 y anteriores utilizan números de compilación hasta r89755, mientras que la versión 10.1.3 y posteriores utilizan números de compilación a partir de 10.2.30.5. Preste atención a la versión del cliente y a los números de compilación cuando consulte estas instrucciones.

Tema principal: Guardium Installation Manager

Instalación del cliente GIM mediante un instalador interactivo: cliente GIM versión 10.1.2 o anteriores

Se proporciona un asistente para ayudarle a instalar el cliente GIM en cada servidor de base de datos.

Procedimiento

1. Coloque el instalador del cliente GIM en cualquier carpeta del servidor de base de datos.
2. Ejecute el archivo setup.exe para iniciar el asistente que instala el cliente GIM. El archivo setup.exe se encuentra en la carpeta Windows_GimClient.
3. Siga las preguntas y responda a las mismas en el asistente de instalación.

Qué hacer a continuación

Puede ver los resultados de la instalación en el archivo de registro en c:\guardiumstaplog.txt.

Instalación del cliente GIM mediante un instalador interactivo: cliente GIM versión 10.1.3 y posteriores

Se proporciona un asistente para ayudarle a instalar el cliente GIM en cada servidor de base de datos.

Procedimiento

1. Coloque el instalador del cliente GIM en cualquier carpeta del servidor de base de datos.
2. Ejecute el archivo setup.exe para iniciar el asistente que instala el cliente GIM. El archivo setup.exe se encuentra en la carpeta GIM-Installer-10.2*.
3. Siga las preguntas y responda a las mismas en el asistente de instalación.

Qué hacer a continuación

Puede ver los resultados de la instalación en el archivo de registro en C:\IBM Windows GIM.ctl..

Instalación del cliente GIM mediante una instalación silenciosa: cliente GIM versión 10.1.2 o anteriores

Si lo prefiere, puede instalar el cliente GIM desde la línea de mandatos en lugar de utilizar el asistente.

Acerca de esta tarea

Procedimiento

1. Coloque el instalador del cliente GIM en cualquier carpeta del servidor de base de datos.
2. Abra un indicador de mandatos y vaya a la carpeta Windows_GimClient bajo la carpeta en la que ha colocado el instalador.
3. Escriba este mandato, sin saltos de línea. `setup.exe /s /z" --host=g10.guardium.com --path=c:\\program files (x86)\\guardium\\GIM --perl=c:\\perl\\bin --localip=192.168.1.100"` Incluya todos los espacios y comillas exactamente tal como se muestra en este ejemplo. Si se eliminan o se añaden espacios, el instalador fallará. El parámetro --perl= indica dónde está instalado Perl en este sistema. Este parámetro es opcional. Si no lo especifica, el instalador instala una instancia de Perl.
   Atención:
   - Omita el parámetro --host para instalar el cliente en modalidad de escucha de GIM. La modalidad de escucha permite que el cliente GIM esté disponible para el registro remoto desde un sistema Guardium. Ejemplo de cómo instalarlo como escucha: setup.exe /s /z"--path=c:\program files (x86)\guardium\GIM --host=GIM_HOST" Para obtener más información, consulte Activación remota de GIM y Creación de un proceso de descubrimiento automático de GIM.
   - Cuando clone servidores de base de datos y establezca despliegues de gran tamaño, utilice --auto_assign_ip=1 para asignar una dirección IP aleatoria de una de las direcciones IP válidas de un servidor de base de datos. No especifique auto_assign_ip y localip cuando instale el cliente GIM. Cuando actualice el parámetro GIM_AUTO_SET_CLIENT_IP mediante Gestionar > Instalación de módulo > Configuración por cliente o Configuración por módulo, debe reiniciar el servicio de cliente GIM para que el nuevo valor entre en vigor.

Qué hacer a continuación

Puede ver los resultados de la instalación en el archivo de registro en c:\guardiumstaplog.txt.

Instalación del cliente GIM mediante la instalación silenciosa: cliente GIM versión 10.1.3 o posteriores

Si lo prefiere, puede instalar el cliente GIM desde la línea de mandatos en lugar de utilizar el asistente.

Procedimiento

1. Coloque el instalador del cliente GIM en cualquier carpeta del servidor de base de datos.
2. Abra un indicador de mandatos y vaya a la carpeta GIM_Installer* bajo la carpeta en la que ha colocado el instalador.
3. Escriba este mandato, sin saltos de línea. `setup.exe -UNATTENDED -INSTALLPATH "c:\Program Files(x86)\Guardium Installation Manager" -LOCALIP 10.9.876.543`
   Atención:
   -
     - Los parámetros UNATTENDED y LOCALIP son obligatorios. APPLIANCE es opcional y, si no se proporciona, se activará la modalidad de escucha. Si se utiliza el parámetro AUTO_ASSIGN_IP, no se necesita LOCALIP.
     - Omita el parámetro -APPLIANCE para instalar el cliente en modalidad de escucha de GIM. La modalidad de escucha permite que el cliente GIM esté disponible para el registro remoto desde un sistema Guardium. Ejemplo de cómo se instala como escucha: setup.exe -UNATTENDED -INSTALLPATH C:\program files (x86)\guardium\GIM -LOCALIP 10.9.876.543. Para obtener más información, consulte Activación remota de GIM y Creación de un proceso de descubrimiento automático de GIM.
     - Cuando clone servidores de base de datos y establezca despliegues de gran tamaño, utilice --auto_assign_ip=1 para asignar una dirección IP aleatoria de una de las direcciones IP válidas de un servidor de base de datos. No especifique auto_assign_ip y localip cuando instale el cliente GIM. Cuando actualice el parámetro GIM_AUTO_SET_CLIENT_IP mediante Gestionar > Instalación de módulo > Configuración por cliente o Configuración por módulo, debe reiniciar el servicio de cliente GIM para que el nuevo valor entre en vigor.
   - **Referencia de instalación de línea de mandatos de GIM de Windows**

Parámetros aplicables a todos los instaladores .NET

Parámetro	Descripción
-UNATTENDED	Instalación silenciosa. No es necesario ningún valor
-UNINSTALL	Desinstalar. No es necesario ningún valor.
-INSTALLPATH	Este es el directorio de instalación. La vía de acceso de instalación predeterminada es "C:\Program Files (x86)\Guardium\Guardium Installation Manager"
-CUSTOMER	Para cambiar el nombre del cliente
-COMPANY	Para cambiar el nombre de la empresa
-SERVICEUSER	Para especificar el usuario bajo el que se ejecutará el servicio
-SERVICEPASSWORD	La contraseña del usuario

Parámetros específicos de los instaladores .NET de GIM

Parámetro	Descripción
-APPLIANCE	Para definir la dirección de dispositivo al que se conecta GIM. Si no se especifica este parámetro, la instalación de GIM se realizará en modalidad de escucha.
-LOCALIP	Es la IP del servidor en el que se está instalando GIM.
-KEY_FILE	Para establecer el archivo de claves en un archivo distinto del predeterminado
-CERT_FILE	Para establecer el archivo de certificados en un archivo distinto del predeterminado
-CA_FILE	Para establecer el archivo de CA en un archivo distinto del predeterminado
-SHARED_SECRET	Para establecer el secreto compartido para el registro con el dispositivo si no se especifica mediante el parámetro -APPLIANCE
-LISTENER_PORT	Establece el puerto de escucha para el registro con el dispositivo si no se utiliza el parámetro -APPLIANCE. El valor predeterminado es 8445.
-AUTO_ASSIGN_IP	Cuando el valor se establece en 1, se asigna automáticamente una IP local y NO se debe especificar mediante -LOCALIP. El valor predeterminado es 0.

Qué hacer a continuación

Puede ver los resultados de la instalación en el archivo de registro en C:\IBM Windows GIM.ctl.

Desinstalación del cliente GIM: cliente GIM versión 10.1.2 o anteriores

Procedimiento

1. Abra un indicador de mandatos y vaya a la carpeta Windows_GimClient* bajo la carpeta en la que ha instalado el cliente.
2. Especifique este mandato: Para Installshield, utilice

   ```
   setup.exe /s /z"--host=g10.guardium.com --remove=true"
   ```

   El parámetro --host= es opcional.

Desinstalación del cliente de GIM: cliente GIM versión 10.1.3 y posteriores

Procedimiento

1. Abra un indicador de mandatos y vaya a la carpeta GIM_Installer* bajo la carpeta en la que ha instalado el cliente.
2. Especifique este mandato:

```
setup.exe -UNINSTALL
```

Instalación del cliente GIM en un servidor UNIX

Utilice este mandato para instalar el cliente GIM en cada servidor de base de datos.

Acerca de esta tarea

A partir de Guardium 9.1, puede instalar y utilizar el cliente GIM en una zona esclava de Solaris o en una partición de carga de trabajo (WPAR) de AIX. Esto le permite utilizar el cliente GIM para instalar un S-TAP en una zona esclava o WPAR. Cuando se instala un S-TAP en una zona esclava o una WPAR, el K-TAP se inhabilita, independientemente del valor del parámetro ktap_enabled. También puede utilizar el cliente GIM para instalar el agente CAS (Configuration Auditing System) en una zona esclava o WPAR. No puede instalar el paquete de descubrimiento en una zona esclava o WPAR; el agente de descubrimiento que se ejecuta en la zona global puede recopilar información de otras zonas. El proceso para instalar el cliente GIM en una zona esclava de Solaris o en una partición de carga de trabajo de AIX es igual que el proceso de instalación en la zona maestra. La instalación puede tardar unos segundos más que la instalación en la zona maestra. Si instala el cliente GIM en un sistema Solaris con zonas maestras y esclavas, debe instalar el cliente en la misma ubicación en las zonas maestras y esclavas. Esta ubicación no puede ser un directorio compartido.

En Solaris, el cliente GIM y el supervisor de cada zona esclava se controlan mediante el proceso supervisor de GIM que se ejecuta en la zona maestra. Si el proceso supervisor de la zona maestra se cierra, todos los procesos de GIM de las zonas esclavas también se cierran.

Nota: GIM requiere al menos 300 MB de espacio de disco y 700 MB si también se instala el módulo FAM.

Procedimiento

1. Coloque el instalador del cliente GIM en cualquier carpeta del servidor de base de datos.
2. Ejecute el instalador: `./<installer_name> [-- --dir <install_dir> <--sqlguardip> <g-machine ip> --tapip <db server ip address> --perl <perl dir> -q]`
   Atención:
   - Omita el parámetro --sqlguardip si desea instalar el cliente en modalidad de escucha de GIM. La modalidad de escucha permite que el cliente GIM esté disponible para el registro remoto desde un sistema Guardium. Para obtener más información, consulte Activación remota de GIM y Creación de un proceso de descubrimiento automático de GIM.
   - Cuando clone servidores de base de datos y establezca despliegues de gran tamaño, utilice --auto_set_gim_tapip para asignar una dirección IP aleatoria de una de las direcciones IP válidas de un servidor de base de datos. No especifique auto_set_gim_tapip y tapip cuando instale el cliente GIM. Actualice el parámetro GIM_AUTO_SET_CLIENT_IP después de la instalación del cliente de GIM utilizando Gestionar > Instalación de módulo > Configuración por cliente o Configuración por módulo.
3. En Red Hat Linux versión 6 o posterior, ejecute estos mandatos para verificar que los archivos se han añadido:

   ```
   ls -la /etc/init/gim*
   ls -la /etc/gsvr*
   ```

   En Solaris versión 10 o posterior, ejecute este mandato:

   ```
   ls /lib/svc/method/guard_g*
   ```

   En las demás plataformas, ejecute estos mandatos para verificar que se han añadido las siguientes entradas nuevas a /etc/inittab:

   ```
   gim:2345:respawn:<perl dir>/perl <modules install dir>/GIM/<ver>/gim_client.pl
   gsvr:2345:respawn:<modules install dir>/perl <modules install dir>/SUPERVISOR/<ver>/guard_supervisor
   ```

   Donde modules install dir es el directorio en el que están instalados todos los módulos de GIM, por ejemplo /usr/local/guardium/modules.
4. Especifique este mandato para verificar que el cliente GIM, el proceso SUPERVISOR y los módulos se están ejecutando:

   ```
   ps -afe | grep modules
   ```

5. Inicie una sesión en el sistema Guardium y compruebe el estado del supervisión de los procesos.

Qué hacer a continuación

Tema principal: Guardium Installation Manager

Desinstalación del cliente GIM

Procedimiento

1. Ejecute este mandato: <GIM installation directory>/GIM/current/uninstall.pl
2. Verifique que <GIM installation directory> se ha eliminado.

Actualización del cliente GIM

Puede utilizar GIM para actualizar el cliente GIM a una versión más reciente.

Procedimiento

1. Suba el archivo BUNDLE-GIM.gim más reciente disponible al sistema Guardium.
2. Utilice la GUI de GIM para planificar la instalación del nuevo archivo BUNDLE-GIM.gim.
3. Supervise el proceso de instalación pulsando en el icono i y luego Renovar. Cuando la instalación haya finalizado correctamente, se mostrará el estado INSTALLED.

Tema principal: Guardium Installation Manager

Utilización de grupos con GIM

Puede utilizar grupos para facilitar algunas tareas de GIM.

Antes de empezar

Acerca de esta tarea

Puede crear un grupo de clientes de GIM y utilizarlo para desplegar actualizaciones en estos servidores gestionados.

Procedimiento

1. Pulse Configuración > Herramientas y vistas > Creador de grupos. En el Creador de grupos, cree un grupo nuevo. Como descripción del tipo de grupo, elija Nombre de host del cliente. El nuevo grupo se añade a la lista de grupos existentes.
2. Elija el nuevo grupo en la lista Modificar grupos existentes y añada miembros al grupo. Puede añadirlos manualmente o llenar la lista a partir de una consulta. Para llenar la lista a partir de una consulta, pulse Cumplimentar desde consulta; tenga en cuenta estos requisitos:
    a. Para Consulta, seleccione un nombre de informe que empiece por GIM.
    b. Para Miembro de captación desde columna, seleccione Nombre de cliente GIM.
    c. En cada campo Especifique (como), escriba el valor que desea comparar o % si este campo no se utiliza para identificar clientes.
    d. Guarde el grupo y ejecute o planifique la consulta.

Resultados

Puede utilizar el grupo en la pantalla Gestionar > Instalación de módulo > Configuración por cliente para trabajar con este conjunto de clientes como un grupo en lugar de hacerlo individualmente.

Tema principal: Guardium Installation Manager

Cómo copiar un módulo K-TAP mediante GIM

Si crea un módulo K-TAP personalizado para un servidor de base de datos Linux, puede utilizar GIM para copiar dicho módulo en otros servidores de base de datos Linux.

Antes de empezar

El módulo K-TAP personalizado se crea cuando se instala un S-TAP en un servidor Linux para el que no hay ningún K-TAP precompilado para el kernel actual. El módulo K-TAP personalizado sólo se crea si se ha instalado el paquete kernel-devel. Cuando instale el lote de S-TAP, utilice la interfaz de usuario de GIM para establecer el valor del parámetro de GIM STAP_UPLOAD_FEATURE en 1. Esto indica al cliente GIM que suba el módulo K-TAP personalizado al sistema Guardium después de que se haya creado y que luego cree automáticamente un lote de S-TAP personalizado.

Procedimiento

1. Utilice GIM para instalar el S-TAP en el servidor de base de datos Linux. El instalador determina que es necesario un módulo K-TAP personalizado y lo crea.
2. El módulo K-TAP personalizado, junto con su valor sha256sum, se sube automáticamente al sistema Guardium para el que se ha configurado el S-TAP. Tenga en cuenta que es posible que sea el sistema Guardium que utiliza como servidor GIM.
3. En el sistema Guardium en el que se ha subido K-TAP, ejecute este mandato de la CLI: grdapi make_bundle_with_uploaded_kernel_module, Esto añade el módulo K-TAP recién creado al lote de S-TAP correspondiente. Debe haber al menos un lote de S-TAP cuyos atributos de número de compilación y sistema operativo coincidan con los del módulo K-TAP subido. Los lotes cargados se almacenan en /var/gim_dist_packages. El script crea un nuevo lote de S-TAP en el que se añade _8XX al número de compilación. El nuevo lote se encuentra en /var/dump. Después de ejecutar el mandato GuardAPI, grdpi make_bundle_with_uploaded_kernel_module, es necesario cargar el nuevo lote de GIM. De lo contrario, no resultará visible en la GUI de GIM. Si el mandato GuardAPI, grdpi make_bundle_with_uploaded_kernel_module, se ejecuta correctamente, se mostrará el siguiente mensaje de ejemplo que contiene el nombre del nuevo lote de STAP: Created guard-bundle-STAP-9.0.0_r71327_v90_800-suse-11-linux-x86_64.gim with kernel ktap-71327-suse-11-linux-x86_64-xCUSTOMxeagle910-3.0.101-303.gefb7031-default-x86_64-SMP. A continuación, ejecute el mandato GuardAPI, grdapi gim_load_package, y especifique el nombre del nuevo lote mostrado en el paso anterior.
4. Si el nuevo lote se encuentra en un sistema Guardium que no es el servidor GIM, copie el nuevo lote en el servidor GIM.
5. Utilice la GUI o la CLI de GIM para distribuir el nuevo lote a otros servidores de base de datos que se ejecuten en la misma distribución de Linux que el servidor en el que se ha creado el K-TAP personalizado. Hay cientos de distribuciones de Linux disponibles, y la lista va en aumento. Esto significa que es posible que aún no haya un K-TAP disponible para su distribución de Linux. Si no está disponible el K-TAP correcto, el proceso de instalación de S-TAP puede crearlo. Cuando cree un nuevo módulo K-TAP para un servidor de base de datos Linux, puede copiar dicho módulo en otros servidores de base de datos que ejecuten la misma distribución de Linux.

Tema principal: Guardium Installation Manager
Copia de un nuevo módulo K-TAP en otros sistemas

Actualización dinámica de GIM

Los clientes GIM comprueban si hay actualizaciones del servidor GIM a intervalos regulares. El servidor GIM puede calcular el mejor intervalo de sondeo a utilizar en función de las condiciones del sistema.

Cada cliente GIM envía un mensaje "alive" a su servidor GIM de forma regular para comprobar si hay actualizaciones listas para ser procesadas. Este intervalo de sondeo se calcula y se actualiza en función de las condiciones del servidor GIM. El intervalo se calcula con regularidad y el nuevo valor se pasa al cliente GIM como respuesta a su mensaje "alive". Esta característica está habilitada de forma predeterminada, pero puede desactivarla si prefiere un intervalo fijo.

En el caso de que un cliente de GIM no pueda conectarse a su servidor GIM después de cinco intentos consecutivos, el cliente de GIM se conecta automáticamente a un servidor de sustitución por anomalía, si se ha especificado uno. El cliente GIM reanuda la conexión con su servidor GIM original cuando dicho servidor vuelve a estar disponible. El servidor GIM y el servidor de sustitución por anomalía se configuran utilizando los parámetros GIM_URL y GIM_FAILOVER_URL, respectivamente.

La actualización dinámica se controla mediante el mandato de la API de Guardium gim_set_global_param, con estos parámetros.

dynamic_alive_enabled
: Control de la característica de actividad dinámica. 1 – habilitada, 0 – inhabilitada. Valor predeterminado = 1

dynamic_alive_check_interval
: El intervalo, en minutos, en el que se vuelve a calcular el intervalo de sondeo. Valor predeterminado = 5

Por ejemplo:

```
grdapi gim_set_global_param dynamic_alive_enabled=0
```

Cuando cada cliente GIM envía su mensaje alive al servidor, el servidor responde con el nuevo intervalo de sondeo, así como con cualquier otra actualización que se haya planificado para dicho cliente.

Estos parámetros eran válidos en la versión 10.0 y se han eliminado de la versión 10.1 y posteriores:

- dynamic_alive_default_load_factor
- dynamic_alive_cpu_level1_threshold
- dynamic_alive_cpu_level2_threshold
- dynamic_alive_db_conn_level1_threshold
- dynamic_alive_db_conn_level2_threshold
- dynamic_alive_cpu_load_sample_time

Tema principal: Guardium Installation Manager

Cuando actualice el sistema operativo del servidor de base de datos

Cuando actualice el sistema operativo del servidor de base de datos, puede dejar que el cliente GIM realice los cambios necesarios en sí mismo y en los módulos instalados por GIM.

Antes de empezar

Consulte la información de http://www-01.ibm.com/support/docview.wss?uid=swg21679002 para ver las opciones que están disponibles en función del nivel del cliente GIM.

Acerca de esta tarea

Es mejor actualizar todos los módulos instalados por GIM lo antes posible después de la actualización, ya sea de forma manual o automática. De forma predeterminada, la opción para actualizar estos módulos automáticamente está inhabilitada. Si desea utilizar la actualización automática, debe configurar el sistema Guardium que actúa como su servidor GIM para dar soporte a esta opción, y debe hacer que los lotes necesarios estén disponibles en este servidor.

Procedimiento

1. Para cada módulo que haya instalado en el servidor de base de datos, localice el paquete GIM que contiene la versión más reciente de este módulo que dé soporte a la nueva versión del sistema operativo. El número de compilación de cada lote debe ser el mismo o mayor que el del lote que está instalado actualmente. Cargue cada lote en el servidor GIM.
2. Utilice el mandato gim_set_global_param para establecer el valor del parámetro global auto_install_on_db_server_os_upgrade en 1. Esto habilita la opción de actualización automática en el servidor GIM.

   ```
   grdapi gim_set_global_param paramName="auto_install_on_db_server_os_upgrade" paramValue="1"
   ```

   De forma predeterminada, este parámetro está establecido en 0, lo que significa que la opción está inhabilitada.
3. Después de completar los demás preparativos, actualice el sistema operativo en el servidor de base de datos.

Resultados

Durante el primer arranque después de la actualización del sistema operativo, el cliente GIM reconoce que el sistema operativo se ha actualizado y, como la opción de actualización automática está habilitada, el cliente realiza estos pasos:

1. Cambia los archivos de configuración para todos los módulos instalados por GIM para dar soporte a los atributos del nuevo sistema operativo.
2. Vuelve a registrar todos los módulos en el servidor GIM con los atributos actualizados.
3. Registra una alerta en el informe GIM_EVENTS que indica que se ha producido una actualización del sistema operativo y lista las acciones que se deben llevar a cabo.

Cuando se vuelven a registrar los módulos, el servidor GIM busca primero un lote que tenga el mismo número de compilación que el lote instalado anteriormente, pero que sea compatible con el sistema operativo actualizado. Si no encuentra un lote de este tipo, busca los lotes más recientes que dan soporte a los nuevos atributos del sistema operativo. Si el servidor no encuentra ningún lote adecuado, emite un mensaje de error. Si el servidor encuentra los lotes adecuados, los planifica para la actualización y ejecuta inmediatamente el proceso de actualización.

Qué hacer a continuación

Consulte los mensajes del informe GIM_EVENTS. Si el servidor GIM notifica que los módulos se han actualizado correctamente, compruebe que los módulos funcionan correctamente, tal como haría después de cualquier actualización.

Si se han escrito mensajes de error en el informe GIM_EVENTS que indiquen que la actualización no se ha realizado correctamente, revise los mensajes de error para obtener ayuda.

Después de completar la actualización planificada del sistema operativo, inhabilite la opción de actualización automática en el servidor GIM. Esto impide que un cliente GIM inicie un proceso de actualización por equivocación.

```
grdapi gim_set_global_param paramName="auto_install_on_db_server_os_upgrade" paramValue="0"
```

Puede volver a habilitar la opción de actualización automática cuando realice otra actualización del sistema operativo.
Tema principal: Guardium Installation Manager

Distribución de lotes de GIM a unidades gestionadas

Puede distribuir lotes de GIM a unidades gestionadas para desplegarlos en los clientes GIM gestionados por dichas unidades gestionadas.

Antes de empezar

Acerca de esta tarea

Si gestiona todos los clientes GIM desde el gestor central, puede desplegar lotes en todos los clientes GIM directamente desde el gestor central. Si gestiona grupos de clientes desde varias unidades gestionadas, puede distribuir los lotes de GIM desde el gestor central a estas unidades gestionadas.

El tiempo necesario para la distribución depende del tamaño de los lotes y de las condiciones de red. En una red con una latencia significativa, las transferencias pueden tardar varias horas.

Procedimiento

1. Copie los lotes que desea distribuir en el directorio /var/gim/dist_packages del gestor central. Todos los archivos de este directorio se distribuirán; no puede seleccionar los lotes que desea distribuir.
2. Elija las unidades gestionadas a las que desea distribuir los lotes.
3. Pulse Distribuir lotes GIM. Los lotes se copian en las unidades gestionadas seleccionadas.

Resultados

Puede instalar los lotes de cada unidad gestionada en los clientes de GIM que gestiona.
Tema principal: Guardium Installation Manager

Eliminación de lotes de GIM no utilizados

Puede eliminar los lotes de GIM del servidor GIM si ya no se utilizan en ningún servidor de base de datos.

Acerca de esta tarea

Esta función le permite mantener el inventario de los lotes de GIM e impedir que se utilice innecesariamente espacio de disco.

Puede utilizar dos mandatos nuevos de la API de Guardium para identificar y eliminar lotes de GIM no utilizados. Lleve a cabo este procedimiento en cada sistema Guardium que actúe como servidor GIM.

Procedimiento

1. Ejecute el mandato gim_list_unused_bundles para identificar los lotes no utilizados para la instalación de FAM. Utilice el parámetro includeLatest para indicar si desea que la lista que devuelve el mandato incluya la versión más reciente de cada lote de GIM. Es posible que tenga lotes que aún no ha distribuido o que desee conservar una versión antigua para poderla volver a instalar si es necesario. Establezca includeLatest en 0 para excluir la última versión no utilizada de cada lote de los resultados del mandato. Establézcalo en 1 para incluir todas las versiones no utilizadas. Este parámetro es obligatorio y no se proporciona ningún valor predeterminado. Por ejemplo:

   ```
   gim_list_unused_bundles includelatest=0
   ```

   El mandato devuelve una lista de lotes de GIM que se encuentran en el servidor GIM pero que no están instalados en ningún servidor de base de datos cuyo cliente GIM trabaje con este servidor GIM.
2. Si el paso 1 identifica algunos lotes no utilizados, utilice el mandato gim_remove_bundle para eliminar cada lote no deseado. Este mandato acepta un único parámetro, bundlePackageName, que identifica el lote que se va a eliminar. Este parámetro es obligatorio y no se proporciona ningún valor predeterminado. Utilice los nombres que devuelve el mandato gim_list_unused_bundles.
   El lote nombrado sólo se elimina si:
   - El nombre especificado en bundlePackageName coincide con el nombre de un único lote de GIM específico.
   - No hay ningún lote de GIM cuyo nombre coincida con bundlePackageName instalado en cualquier servidor de base de datos cuyo cliente GIM funcione con este servidor GIM.

   Por ejemplo:

   ```
   gim_remove_bundle bundlePackageName=name
   ```

   donde name es un nombre de lote que ha devuelto el mandato gim_list_unused_bundles.

Resultados

Los lotes de GIM que no se necesitan se eliminan del servidor GIM.
Tema principal: Guardium Installation Manager

Ejecución de diagnósticos de GIM

Puede ejecutar diagnósticos en los clientes GIM para verificar que el servidor GIM tiene datos exactos sobre cada cliente.

Acerca de esta tarea

Si tiene problemas con un cliente GIM, el primer paso debe ser para verificar que el servidor GIM tiene datos precisos sobre dicho cliente. La ejecución de diagnósticos de GIM verifica que los módulos listados para ese cliente en el servidor GIM coinciden con los módulos instalados en el cliente y que los parámetros almacenados en el cliente GIM coinciden con los almacenados en el servidor GIM.

Puede ejecutar los diagnósticos de GIM desde la interfaz de usuario de Guardium o desde la línea de mandatos. Para ejecutarlos desde la línea de mandatos, utilice este mandato:

```
grdapi gim_run_diagnostics clientIP=xx.xx.xx.xx
```

El valor de clientIP puede ser una dirección IP o un nombre de host. Debe ejecutar el mandato en el sistema Guardium que constituye el servidor GIM para este cliente.

Para ejecutar los diagnósticos de GIM desde la GUI, utilice este procedimiento:

Procedimiento

1. Utilice los recuadros de selección situados junto a cada cliente para elegir los clientes para los que desea ejecutar los diagnósticos de GIM.
2. Pulse Ejecutar diagnósticos. La próxima vez que cada cliente sondee el servidor GIM para ver si hay actualizaciones, recibirá el mandato de diagnóstico y lo ejecutará inmediatamente.

Resultados

Puede consultar los resultados en el informe GIM_EVENTS.
Tema principal: Guardium Installation Manager

Depuración de operaciones de GIM

Es posible que tenga que activar la depuración para resolver un problema.

Acerca de esta tarea

Siga estos pasos para activar la depuración de GIM en el servidor GIM (sistema Guardium).

Procedimiento

1. Edite el archivo de propiedades de GIM: /usr/local/jakarta-tomcat-4.1.30/webapps-http/ROOT/WEB-INF/conf/gimserver.log4j.properties.
2. Cambie el valor ERROR por DEBUG.
3. Guarde el archivo.

Resultados

La depuración se activará en unos segundos y los mensajes de depuración se escribirán en el archivo de registro de depuración diario situado en /var/log/guard/debug-logs/.

Qué hacer a continuación

Cuando haya terminado la depuración, vuelva a editar el archivo y cambie DEBUG por ERROR.

Tema principal: Guardium Installation Manager

Habilitación de la depuración del cliente GIM

Acerca de esta tarea

Para habilitar la depuración en el cliente GIM, cambie el parámetro module_DEBUG por 1, donde module es el nombre del módulo instalado cuya operación desea depurar. Puede modificar el parámetro mediante la CLI o la interfaz de usuario. Establezca el valor en 0 cuando finalice la depuración.

Reinicio del supervisor para Solaris con soporte de SMF

Utilice un conjunto de mandatos de la CLI para reiniciar el supervisor en servidores Solaris con soporte de SMF.

Acerca de esta tarea

Para reiniciar el supervisor, siga el procedimiento siguiente. Utilice este procedimiento únicamente en servidores Solaris con soporte de SMF.

Procedimiento

1. Detenga el supervisor con el mandato svcadm -v disable guard_gsvr.
2. Ejecute el mandato svccfg delete -f guard_gsvr.
3. Reinicie el supervisor con el mandato svccfg import <gim install dir> /SUPERVISOR/current/guard_gsvr.xml, donde <gim install dir> es la vía de acceso de archivo al directorio de instalación de GIM.

Resultados

El supervisor se reinicia para Solaris con soporte de SMF.
Tema principal: Guardium Installation Manager

Instalación del sistema Guardium

Este documento describe los pasos necesarios para instalar y configurar el sistema IBM Security Guardium .

Este documento también proporciona información sobre cómo personalizar el particionamiento en el dispositivo y cómo realizar la instalación en una unidad remota (SAN).

Los pasos son los siguientes:

1. Antes de empezar, ensamble la información de configuración y el hardware necesario.
2. Configure el dispositivo físico o el dispositivo virtual.
3. Instale la imagen de Guardium.

4. Establezca la configuración inicial y básica.
5. Verifique la instalación se ha realizado correctamente.

La solución IBM Security Guardium está disponible como:

- Oferta de hardware: Una solución de software totalmente configurada que se proporciona en dispositivos físicos proporcionados por IBM®.
- Oferta de software: La solución se entrega como imágenes de software que despliegan los clientes en su propio hardware, ya sea directamente o como dispositivos virtuales.

Los requisitos listados en este documento se aplican a la instalación tanto del dispositivo físico como del dispositivo virtual, a menos que se especifique lo contrario.

- Modalidades operativas
  Puede desplegar un sistema Guardium en cualquiera de las diferentes modalidades operativas.
- Claves de licencia
  Para establecer un sistema Guardium funcional es necesaria una licencia base y una o varias licencias de adición.
- Requisitos de hardware
  Puede encontrar los requisitos de hardware detallados y las recomendaciones de tamaño en el portal de soporte de IBM.
- Requisitos de los puertos de Guardium
  Cada sistema Guardium debe tener puertos disponibles para varios tipos de comunicaciones. Esta tabla lista estas conexiones y los números de puertos predeterminados asignados.
- Paso 1. Ensamblar lo siguiente antes de comenzar
  Para preparar el despliegue del sistema Guardium, el administrador de la red debe proporcionar la información siguiente.
- Paso 2. Configurar el dispositivo físico o virtual
  Las instrucciones de configuración de esta sección son diferentes cuando se instala en un dispositivo físico o en un dispositivo virtual.
- Paso 3. Instalar la imagen de Guardium
  En esta sección se describe cómo instalar la imagen y particionar el disco.
- Paso 4. Establecer la configuración inicial y básica
  El paso inicial debe ser la configuración de red, el cual se debe realizar localmente a través de la interfaz de línea de mandatos (CLI) accesible a través del puerto serie o de la consola del sistema.
- Paso 5. Qué hacer a continuación
  Esta sección describe los pasos para verificar la instalación, instalar las claves de licencia e instalar cualquier parche de mantenimiento disponible.
- Crear la imagen virtual
  Utilice esta sección para instalar la imagen virtual.
- Particionamiento personalizado
  Si personaliza el particionamiento de la unidad de disco duro, debe realizar varias elecciones.
- Cómo realizar una partición con un LVM cifrado
  Si desea utilizar un disco cifrado, siga estos pasos para crear un volumen LVM cifrado que contenga los volúmenes lógicos / y /var.
- Ejemplo de configuración de SAN
  Este apéndice describe los pasos necesarios para pasar a un indicador de mandatos para realizar una partición previa de una unidad de disco duro (como es necesario para la instalación de SAN).

Modalidades operativas

Puede desplegar un sistema Guardium en cualquiera de las diferentes modalidades operativas.

A medida que planifica su entorno de Guardium, es posible que despliegue sistemas en cualquier o en todas estas modalidades operativas:

Recopilador
: Un recopilador recibe datos sobre las actividades de base de datos o las actividades de archivos de los agentes que se han desplegado en servidores de base de datos y servidores de archivos. El recopilador procesa estos datos y responde según las políticas instaladas en el recopilador. Un recopilador puede exportar datos a un agregador.

Agregador
: Un agregador recopila datos de varios recopiladores para proporcionar una vista agregada de los datos. El agregador no está conectado directamente a servidores de archivos y servidores de bases de datos. Puede asignar recopiladores a agregadores, en función de su ubicación o su función. Por ejemplo, es posible que desee conectar los recopiladores que supervisan los servidores de bases de datos de recursos humanos a un solo agregador, para poder ver los datos relacionados con todos esos servidores en una sola ubicación. Si lo desea, puede implementar un segundo nivel de agregación desplegando un agregador que recopile datos de todos los demás agregadores, en lugar de los de los recopiladores.
  Nota: Si tiene previsto utilizar el dispositivo como un gestor central, DEBE seleccionar la opción Agregador.

Gestor central
: Solo existe un gestor central en un entorno de Guardium, aunque se puede designar otro sistema Guardium como un gestor central de copia de seguridad. Puede utilizar el gestor central para definir políticas y distribuirlas a todos los recopiladores, para realizar otras tareas de configuración que afectan a todos los sistemas Guardium y para realizar varias otras tareas administrativas desde una única consola. El gestor central también puede funcionar como un agregador, recopilando datos de los recopiladores o de otros agregadores. Este modelo proporciona una vista de las actividades para toda la empresa y le permite ver informes basados en datos agregados desde todos los sistemas Guardium.

El número de servidores de archivos y servidores de bases de datos supervisados que se asignan a un recopilador depende de la cantidad de datos que fluyen desde los servidores al recopilador. Para obtener información sobre cuántos recopiladores y agregadores necesita su entorno y cómo ubicar los sistemas Guardium para obtener mejores resultados, consulte la Guía de despliegue para IBM Guardium.

Si está utilizando el componente Asesoramiento de vulnerabilidades de Guardium, debe decidir dónde ha de ejecutar las pruebas de evaluación. Algunos clientes dedican un sistema Guardium separado a esta función. También puede ejecutar pruebas desde cualquier sistema Guardium que se despliega como un recopilador, un agregador o un gestor central.

Tema principal: Instalación del sistema Guardium

Claves de licencia

Para establecer un sistema Guardium funcional es necesaria una licencia base y una o varias licencias de adición.

A continuación se describen las licencias base y las licencias de adición:

- Las claves de licencias base (también conocidas como claves de restablecimiento) reflejan el tipo de máquina del sistema. Por ejemplo, para establecer el sistema recopilador se requiere una licencia base de recopilador.
- Las claves de licencias de adición habilitan conjuntos de características específicos. Por ejemplo, las características típicas de supervisión de actividad de datos requieren una licencia de adición estándar DAM. Se pueden instalar varias licencias de adición combinadas para habilitar la funcionalidad de Guardium.

Cuando se aplica una licencia base, se comprueba el tipo de máquina para verificar la compatibilidad. Hay dos tipos de licencias base:

Tabla 1. Tipos de licencias base

Tipo de licencia base	Descripción de la licencia
Recopilador	Las licencias base de recopilador son válidas para establecer un sistema autónomo o un recopilador.
Agregador	Las licencias base de agregador son válidas cuando se establece un agregador o un sistema de gestor central.

Las características disponibles en el sistema Guardium dependen de las licencias de adición que haya instalado. Las siguientes licencias de adición están disponibles y se pueden combinar:

Tabla 2. Tipos de licencias de adición

Tipo de licencia de adición	Descripción de la licencia
DAM Express	Funcionalidad predefinida para la supervisión de la actividad de datos.
DAM Estándar	Funcionalidad principal para la supervisión de la actividad de datos.
DAM Avanzada	Funcionalidad DAM estándar más control de acceso preciso, enmascaramiento, cuarentena y bloqueo (terminación de actividad).
FAM Estándar	Funcionalidad principal para la supervisión de la actividad de archivos.
FAM Avanzado	Funcionalidad de FAM Estándar más bloqueo.
VA Estándar	Asesoramiento de vulnerabilidades más DPS (Database Protection Service), CAS (Change Audit System) y generación de informes de titularidad de base de datos.

Para obtener información sobre cómo instalar licencias de Guardium, consulte la sección Instalación de las claves de licencia.

Tema principal: Instalación del sistema Guardium
Tareas relacionadas:
Instalación de las claves de licencia

Requisitos de hardware

Puede encontrar los requisitos de hardware detallados y las recomendaciones de tamaño en el portal de soporte de IBM.

Para obtener las especificaciones de hardware detalladas y las recomendaciones, consulte el documento siguiente: IBM Guardium V10.1 Requisitos técnicos de dispositivos de software.

Tema principal: Instalación del sistema Guardium

Requisitos de los puertos de Guardium

Cada sistema Guardium debe tener puertos disponibles para varios tipos de comunicaciones. Esta tabla lista estas conexiones y los números de puertos predeterminados asignados.

Puertos abiertos

Los Puertos utilizados en y por el sistema Guardium.

Servidor de BD: Recopilador

TCP 8443: Abierto desde el servidor de BD al recopilador

TCP 16016: STAP de Unix, ambas direcciones, registro, latido y datos (incluido el S-TAP de IBM i en ejecución en PASE)

TCP 16017: CAS de Windows/Unix, ambas direcciones, plantillas y datos

TCP 16018: STAP (TLS) de Unix, ambas direcciones, registro, latido y datos

TCP 16019: CAS (TLS) de Windows/Unix, ambas direcciones, plantillas y datos

TCP 16020: Desde agente STAP, Borrar agrupación de conexiones STAP de UNIX

TLS 16021: Desde agente STAP, Agrupación de conexiones STAP de UNIX cifradas

TCP 8081: Guardium Installation Manager, ambas direcciones, servidor de bases de datos a recopilador/gestor central

TCP 9500: Windows STAP, ambas direcciones, Servidor de BD a recopilador, Registro de STAP y datos

TCP 9501: Windows STAP (TLS), ambas direcciones, Servidor de BD a recopilador, Registro de STAP y datos

Recopilador: Agregador (Secure Shell – SSL)

TCP 22: Recopilador a agregador, exportaciones de datos SCP, ambas direcciones

Gestor central: Dispositivos gestionados

TCP 22: Transferencias de datos SSH/SCP, ambas direcciones

TCP 8443: SSL, ambas direcciones

TCP 8444: SSL, subida de archivos de STAP a GIM

TCP 3306: MySQL, abierto a fuentes específicas (por ejemplo, el Gestor central está abierto a todas las unidades gestionadas; una unidad gestionada está abierta al Gestor central)

TLS 8447: Se utiliza para la infraestructura del servicio de mensajería remoto (y la infraestructura de distribución de perfiles) para las comunicaciones entre los sistemas Guardium del entorno federado y del entorno gestionado centralmente. Los perfiles de configuración permiten definir los valores de configuración y planificación desde un gestor central y distribuyen de forma práctica estos valores a los grupos de unidades gestionadas sin alterar la configuración del propio gestor central.

FAM (File Activity Monitoring)

TCP/TLS 16022/16023: Canal de información universal. 16022 (supervisión FAM, sin cifrar) y 16023 (supervisión FAM, cifrada), ambos necesitan bidireccionalidad abierta. Sniffer necesita el bloque de bidireccionalidad abierta desde 16016 a 16023.

18087: Puerto de escucha para FAM en el servidor ICM (IBM Content Classification) que se encuentra en la misma máquina en que se ha instalado FAM. (serverSettings.icmURL=http://localhost:18087) Bidireccionalidad abierta.

GIM (Guardium Installation Manager)

8445: Escucha del cliente GIM, ambas direcciones. El cliente de GIM realiza la escucha. Cualquier servidor GIM en el gestor central o en el recopilador puede conectar con el cliente GIM.

8446: TLS autenticado de GIM, ambas direcciones. Se utiliza entre el cliente GIM y el servidor GIM (en el gestor central o el recopilador). Si el valor de GIM_USE_SSL NO está inhabilitado, gim_client intenta comunicar su certificado a través del puerto 8446. Si el puerto 8446 NO está abierto, se toma el valor predeterminado 8444, PERO no se pasa ningún certificado (por ejemplo, TLS sin verificación).

8081: TLS, para utilizar 8081 para que el cliente GIM se conecte al servidor GIM, es necesario inhabilitar el parámetro GIM_USE_SSL. Su valor predeterminado es ON. Este parámetro forma parte de los parámetros comunes de GIM en la GUI. Si el valor de GIM_USE_SSL NO está inhabilitado, gim_client intenta comunicar su certificado a través del puerto 8446. Si el puerto 8446 NO está abierto, se toma el valor predeterminado 8444, PERO no se pasa ningún certificado (por ejemplo, TLS sin verificación).

Equilibrador de carga empresarial

TLS 8443: Equilibrador de carga empresarial S-TAP, es necesario para que los S-TAP de UNIX/Linux comuniquen las instancias al recopilador. No obstante, este puerto también lo utiliza el equilibrador de carga del gestor central. S-TAP inicia una solicitud al gestor central (equilibrador de carga) en 8443, enviando el mensaje de HTTPS, si la instalación indica que se ha de utilizar el equilibrador de carga. Entre el servidor de bases de datos y el gestor central, se puede utilizar un servidor proxy, si el cliente no desea un puerto abierto directamente desde la base de datos al Gestor central.

Búsqueda rápida para empresa

TCP 8983: SOLR - De entrada, SSL

TCP 9983: SOLR - De entrada, SSL

Interfaz de usuario: Sistema Guardium (autónomo, agregador, gestor central)

TCP 22: Usuario a sistema, conectividad de CLI, ambas direcciones

TCP 8443: Usuario a sistema, conectividad de GUI (configurable), ambas direcciones

System: Servidor SMTP

TCP 25: sistema a servidor SMTP, alertas de correo electrónico

System: Servidor SNMP

UDP 161: Cliente SNMP a sistema. Sondeo SNMP

UDP 162: Sistema a servidor SNMP, excepciones SNMP

System: Servidor SYSLOG

UDP/TCP 514: Mensaje de syslog remoto desde/a otros sistemas, normalmente SIEM. **Nota:** El puerto local es 514, pero el número de puerto remoto se de especificar en la configuración. Si se utiliza el cifrado, el protocolo debe ser TCP, no UDP.

System: Servidor NTP

TCP/UDP 123: Sistema a NTPS (Network Time Protocol Server)

System: Servidor DNS

TCP/UDP 53: Sistema a servidor de nombres de dominio

System: EMC Centera (copias de seguridad)

TCP 3218: Sistema a EMC Centera

System: Tivoli LDAP

UDP 389: sistema a/desde Tivoli LDAP

System: Sistema principal

TCP 16022: Conecta S-TAP con DB2 z/OS, S-TAP IMS, S-TAP VSAM (conjunto de datos S-TAP)

TCP 16023: Conexiones TLS, específicamente AT-TLS (Application Transparent Transport Layer Security) de IBM

Puertos para las conexiones con los servidores de base de datos de Windows

Puerto	Protocolo	Finalidad
8075	UDP	Señal de latido de S-TAP de Windows (tráfico bidireccional). Nota: El agente S-TAP de UNIX no utiliza UDP para señales de latido, por lo tanto no existe un puerto UNIX correspondiente para esta función.
9500	TCP	Borrar S-TAP de Windows
9501	TLS	S-TAP de Windows cifrado (opcional)
16017	TCP	Borrar CAS de Windows
16019	TLS	CAS de Windows cifrado (opcional)

Puertos predeterminados utilizados para el acceso de aplicaciones Guardium

Puerto	Protocolo	Finalidad
8443	TCP	Acceso de navegador web (https) a la interfaz de usuario de Guardium. Nota: Este puerto lo puede cambiar el administrador de Guardium , también se utiliza para registrar una unidad gestionada en el gestor central.
22	TCP	Acceso SSH desde clientes para gestionar el dispositivo Guardium.
3306	TCP	Comunicación entre el gestor central y las unidades gestionadas

Puertos para las conexiones con los servidores de base de datos de z/OS

Puerto	Protocolo	Finalidad
16022	TCP	Se conecta con S-TAP para DB2 z/OS, S-TAP para IMS, S-TAP para conjuntos de datos
16023	TCP	Conexiones TLS, específicamente AT-TLS (Application Transparent Transport Layer Security) de IBM
41500	TCP	Puerto inicial predeterminado para las comunicaciones de registro de mensajes internos: LOG_PORT_SCAN_START
39987	TCP	Puerto predeterminado de las comunicaciones específicas del agente, entre el agente y los espacios de direcciones secundarios del agente: ADS_LISTENER_PORT

Puertos predeterminados utilizados para otras características

Puerto	Protocolo	Finalidad
20, 21	TCP	Servidor FTP para copia de seguridad/archivado (opcional)
22	TCP	SCP para copia de seguridad/archivado, distribuciones de parches y transferencias de archivos
25	TCP	SMTP (servidor de correo electrónico) para alertas y otras notificaciones
53	TCP	Servidores DNS
123	TCP, UDP	NTP (Servidor de tiempo) para sincronización horaria
161	TCP, UDP	Sondeo SNMP (opcional)

162	TCP, UDP	Excepciones SNMP (opcional)
389	TCP	LDAP, por ejemplo, Active Directory o Sun One Directory
514	TCP	Servidor syslog (opcional)
636	TCP	LDAP, por ejemplo, Active Directory o Sun One Directory sobre SSL (opcional)
1500	TCP	Hosts de copia de seguridad de Tivoli Storage Manager (opcional)
3218	TCP, UDP	Hosts de copia de seguridad de EMC Centera (opcional)
definido por el usuario	TCP	Puertos de escucha de servidor de base de datos, por ejemplo, 1521 para Oracle o 1433 para MS-SQL, para el acceso de origen de datos de Guardium (opcional)
16022/16023	TCP/TLS	Canal de información universal: File Activity Monitoring FAM0
18027		FAM utilizando localmente IBM Content Classification (serverSettings.icmURL=http://localhost:18087)
8445		Escucha de cliente GIM, ambas direcciones El cliente de GIM realiza la escucha. Cualquier servidor GIM en el gestor central o en el recopilador puede conectar con el cliente GIM.
8446	TLS	TLS autenticado por GIM, ambas direcciones Se utiliza entre el cliente GIM y el servidor GIM (en el gestor central o el recopilador). Si el valor de GIM_USE_SSL NO está inhabilitado, gim_client intenta comunicar su certificado a través del puerto 8446. Si el puerto 8446 NO está abierto, se toma el valor predeterminado 8444, PERO no se pasa ningún certificado (por ejemplo, TLS sin verificación).
8447	TLS	Se utiliza para la infraestructura del servicio de mensajería remoto (y la infraestructura de distribución de perfiles) para las comunicaciones entre los sistemas Guardium del entorno federado y del entorno gestionado centralmente. Los perfiles de configuración permiten definir los valores de configuración y planificación desde un gestor central y distribuyen de forma práctica estos valores a los grupos de unidades gestionadas sin alterar la configuración del propio gestor central.
8443	TLS	Equilibrador de carga empresarial Es necesario para que los S-TAP de UNIX/Linux comuniquen las instancias al recopilador. No obstante, este puerto también lo utiliza el equilibrador de carga del gestor central. Si la instalación desea utilizar el equilibrador de carga empresarial, S-TAP inicia una solicitud para el gestor central en el puerto 8443, enviando un mensaje HTTPS. De modo que entre el servidor de bases de datos y el gestor central, se puede utilizar un servidor proxy, si el cliente no desea un puerto abierto directamente desde la base de datos al Gestor central.
8081	TLS	Para utilizar 8081 para que el cliente GIM se conecte al servidor GIM, es necesario inhabilitar el parámetro GIM_USE_SSL. Su valor predeterminado es ON. Este parámetro forma parte de los parámetros comunes de GIM en la GUI. Si el valor de GIM_USE_SSL NO está inhabilitado, gim_client intenta comunicar su certificado a través del puerto 8446. Si el puerto 8446 NO está abierto, se toma el valor predeterminado 8444, PERO no se pasa ningún certificado (por ejemplo, TLS sin verificación).
8983	TCP	SOLR, de entrada, SSL (Búsqueda rápida para empresa)
9983	TCP	SOLR, de entrada, SSL (Búsqueda rápida para empresa)

Tema principal: Instalación del sistema Guardium

Paso 1. Ensamblar lo siguiente antes de comenzar

Para preparar el despliegue del sistema Guardium, el administrador de la red debe proporcionar la información siguiente.

- La dirección IP de la tarjeta de interfaz (eth0)
- La máscara de subred para la dirección IP primaria
- La dirección IP del direccionador predeterminado.
- El nombre de host y el nombre de dominio que se va a asignar al sistema
- Las direcciones IP DNS (hasta tres direcciones) y añadir el nuevo sistema Guardium a su dominio DNS
- (opcional) La dirección IP para la interfaz de gestión secundaria
- (opcional) La máscara para la interfaz de gestión de IP secundaria
- (opcional) La pasarela para la interfaz de gestión de IP secundaria
- (opcional) Nombre de host del servidor NTP
- (opcional) La información de configuración de SMTP (para alertas de correo electrónico): La dirección IP, puerto y si se utiliza la autenticación, un nombre de usuario y una contraseña de SMTP
- (opcional) La información de configuración de SNMP (para alertas SNMP) la dirección IP del servidor SNMP y el nombre de comunidad de la excepción que se va a utilizar.

- Dispositivos de almacenamiento SAN
  Si la instalación se va a desplegar en una red de área de almacenamiento (SAN), toda la información de configuración que necesita la SAN, debe estar preparada antes del despliegue. Asimismo, hay pasos de instalación adicionales que son necesarios para la partición del dispositivo de almacenamiento SAN y la instalación del SO de Guardium.

Tema principal: Instalación del sistema Guardium

Dispositivos de almacenamiento SAN

Si la instalación se va a desplegar en una red de área de almacenamiento (SAN), toda la información de configuración que necesita la SAN, debe estar preparada antes del despliegue. Asimismo, hay pasos de instalación adicionales que son necesarios para la partición del dispositivo de almacenamiento SAN y la instalación del SO de Guardium.

Nota: Se da soporte a la instalación en SAN. La instalación en NAS no está soportada.
Tema principal: Paso 1. Ensamblar lo siguiente antes de comenzar

Paso 2. Configurar el dispositivo físico o virtual

Las instrucciones de configuración de esta sección son diferentes cuando se instala en un dispositivo físico o en un dispositivo virtual.

- Dispositivo físico
  Después de que se haya cargado el dispositivo en el bastidor del cliente, conecte el dispositivo a la red de la siguiente manera:
- Cómo identificar eth0 y otros puertos de red
  Utilice los siguientes mandatos de CLI para correlacionar los puertos de red.
- Contraseñas predeterminadas para dispositivos físicos
  Se proporcionan contraseñas predeterminadas para usuarios predefinidos.
- Dispositivo virtual
  La máquina virtual (MV) de IBM Security Guardium es una solución solo de software con licencia que se instala en una máquina virtual huésped, tal como VMware ESX Server.

Tema principal: Instalación del sistema Guardium

Dispositivo físico

Después de que se haya cargado el dispositivo en el bastidor del cliente, conecte el dispositivo a la red de la siguiente manera:

1. Busque las conexiones de alimentación. Enchufe el cable o los cables de alimentación adecuados a estas conexiones.
2. Conecte el cable de red al puerto de red eth0. Conecte cualquier cable de red secundario opcional.
3. Conecte un teclado, vídeo y ratón directamente o mediante una conexión KVM (ya sea a través del puerto USB o a través del puerto USB) al sistema.
4. Encienda el sistema.

Tema principal: Paso 2. Configurar el dispositivo físico o virtual
Información relacionada:
Guía de instalación y servicio de Lenovo System x3550 M5
Documento de requisitos técnicos
Cambios del puerto de gestión eth0

Cómo identificar eth0 y otros puertos de red

Utilice los siguientes mandatos de CLI para correlacionar los puertos de red.

show network interface inventory

Utilice este mandato de CLI para visualizar los nombres de puertos y las direcciones MAC de todas las interfaces de red instaladas.

```
show network interface inventory
eth0 00:13:72:50:CF:40
eth1 00:13:72:50:CF:41
eth2 00:04:23:CB:11:84
eth3 00:04:23:CB:11:85
eth4 00:04:23:CB:11:96
eth5 00:04:23:CB:11:97
```

show network interface port

Utilice este mandato de CLI para ubicar un conector físico en la parte posterior del dispositivo. Después de utilizar el mandato show network interface inventory para visualizar todos los nombres de puertos, utilice este mandato para que parpadee el piloto del puerto físico especificado mediante n (el dígito que sigue a *eth*: eth0, eth1, eth2, eth3, etc), 20 veces.

```
show network interface port 1
```

El indicador del puerto eth1 parpadeará 20 veces.

Instale el software directamente en el sistema dedicado

Cuando instale el software de Guardium directamente en el disco de un sistema dedicado, utilice las instrucciones del dispositivo físico.

Tema principal: Paso 2. Configurar el dispositivo físico o virtual

Contraseñas predeterminadas para dispositivos físicos

Se proporcionan contraseñas predeterminadas para usuarios predefinidos.

Cuando reciba un dispositivo físico de IBM, utilice estas contraseñas para la configuración inicial.
Nota: Asegúrese de cambiar todas las contraseñas predeterminadas cuando haya finalizado la instalación.

Tabla 1. Contraseñas predeterminadas para usuarios predeterminados

Usuario	Contraseña predeterminada
accessmgr	guard1accessmgr
admin	guard1admin
cli	guard1cli

Tema principal: Paso 2. Configurar el dispositivo físico o virtual

Dispositivo virtual

La máquina virtual (MV) de IBM Security Guardium es una solución solo de software con licencia que se instala en una máquina virtual huésped, tal como VMware ESX Server.

Para instalar la MV de Guardium, siga los pasos de la sección Crear la imagen virtual. Los pasos son los siguientes:

- Verificar la compatibilidad del sistema
- Instalar VMware ESX Server
- Conectar cables de red
- Configurar el portal de gestión de MV
- Crear una nueva máquina virtual
- Instalar el dispositivo virtual de IBM Security Guardium.

Después de instalar la MV, vuelva al paso 4, Establecer la configuración inicial y básica, para obtener instrucciones adicionales acerca de cómo configurar el sistema Guardium.

Tema principal: Paso 2. Configurar el dispositivo físico o virtual

Paso 3. Instalar la imagen de Guardium

En esta sección se describe cómo instalar la imagen y particionar el disco.

1. Asegúrese de que los valores de la secuencia de arranque de UEFI/BIOS se hayan establecido de modo que el arranque se intente desde el soporte extraíble (la unidad de CD/DVD) antes de utilizar la unidad de disco duro.
   Nota: La instalación puede realizarse desde el DVD. Si es necesario, solicite la contraseña de UEFI/BIOS al soporte técnico.
2. Cargue la imagen de Guardium desde el DVD de instalación.
3. Se muestran las dos opciones siguientes:

   Instalación estándar: Este es el valor predeterminado. Utilice esta opción en la mayoría de los casos para particionar el disco.

   Instalación de partición personalizada: Permite una mayor personalización de todas las particiones (localmente o en un disco SAN). Consulte el apartado Particiones personalizadas para obtener más información sobre cómo implementar esta opción.

   Nota:
   - La instalación estándar limpia el disco, vuelve a particionar y formatear el disco e instala un nuevo sistema operativo.
   - En el primer arranque después de la instalación, se le solicita al usuario que acepte un acuerdo de licencia. Puede utilizar Avance de página para leer el acuerdo o Q para saltar al final. Para aceptar los términos del acuerdo, escriba `q` para salir y, a continuación, escriba `yes`. El usuario debe especificar `yes` en el acuerdo o la máquina no arrancará.
4. El sistema arranca desde el DVD. Esta instalación tarda unos 12 minutos.

   (d) El proceso de instalación le pedirá ahora que seleccione un recopilador o agregador (se establece en "Recopilador" automáticamente transcurridos 10 segundos si no se proporciona ninguna entrada). Consulte la sección de visión general del producto para obtener una descripción del recopilador y el agregador. Si desea seleccionar el agregador y no lo hace en 10 segundos, debe volver a instalar para poder regresar al punto exacto en que tiene la opción de agregador.

   Nota: Si tiene previsto utilizar el dispositivo como un gestor central, DEBE seleccionar la opción Agregador.
5. El sistema se reinicia automáticamente en este punto para completar la instalación. El primer inicio de sesión después del reinicio requiere cambiar las contraseñas.

Tema principal: Instalación del sistema Guardium

Paso 4. Establecer la configuración inicial y básica

El paso inicial debe ser la configuración de red, el cual se debe realizar localmente a través de la interfaz de línea de mandatos (CLI) accesible a través del puerto serie o de la consola del sistema.

Entre la contraseña *cli* temporal que ha proporcionado anteriormente.

En los pasos siguientes, proporcionará varios parámetros de red para integrar el sistema Guardium en el entorno, utilizando mandatos de CLI.

En la sintaxis de CLI, se indican las variables con estos signos: <dirección_ip>

Sustituya cada variable por el valor adecuado para su red y su instalación. No incluya los corchetes.

- Establecer la dirección IP del sistema primario
  La dirección IP primaria es para la conexión eth0, y se define utilizando los dos mandatos siguientes:
- Establecer la dirección IP predeterminada del direccionador
  Utilice el siguiente mandato de CLI:
- Establecer la dirección IP del servidor DNS
  Establezca la dirección IP de uno o varios servidores DNS que utilizará el dispositivo para resolver los nombres de host y las direcciones IP. Se requiere el primer resolvedor, los otros son opcionales.
- Servidor SMTP
  Es necesario un servidor SMTP para enviar alertas del sistema. Especifique los mandatos siguientes para establecer la dirección IP del servidor SMTP, establecer una dirección de retorno para los mensajes y habilitar las alertas SMTP al arrancar.
- Establecer el nombre de host y el nombre de dominio
  Configure el nombre de host y el nombre de dominio del dispositivo. Este nombre debe coincidir con el nombre de host registrado para el dispositivo en el servidor DNS.
- Establecer el huso horario, la fecha y la hora
  Hay opciones para establecer la fecha y hora del dispositivo.
- Establecer el tipo de unidad inicial
  Un dispositivo puede ser una unidad autónoma, un gestor o una unidad gestionada. Además, se puede establecer un dispositivo para capturar la actividad de la base de datos a través de la inspección de red o S-TAP o ambas cosas. La configuración estándar será para un dispositivo autónomo (para todos los dispositivos), y el valor más común utilizará la captura S-TAP (sólo para los recopiladores).
- Restablecer la contraseña root
  Restablezca su contraseña root en el dispositivo utilizando su propia passkey privada mediante el siguiente mandato de CLI (requiere la clave de acceso *"t0Tach"*):
- Validar todos los valores
  Antes de cerrar sesión en la CLI y pasar al siguiente paso de configuración, revise y valide los valores configurados, utilizando los siguientes mandatos:
- Rearrancar el sistema
  Si el sistema no está en su ubicación final, ahora es un buen momento para concluir el sistema, colocarlo en su ubicación final de red e iniciarlo de nuevo.

Tema principal: Instalación del sistema Guardium

Establecer la dirección IP del sistema primario

La dirección IP primaria es para la conexión eth0, y se define utilizando los dos mandatos siguientes:

```
store network interface ip <dirección_ip>
store network interface mask <máscara_subred>
```

La máscara de interfaz de red es 255.255.255.0. Si este valor es la máscara correcta para la red, puede omitir el segundo mandato.

Para asignar una dirección IP secundaria, utilice el mandato de CLI, store network interface secondary [on <interface> <ip> <mask> <gw> | off], que se puede utilizar para habilitar/inhabilitar la interfaz secundaria.

A continuación, debe reiniciar la red utilizando el mandato de CLI, restart network. No puede asignar una dirección IP secundario mediante la GUI, solo puede hacerlo con la CLI.

Se pueden utilizar las tarjetas de interfaz de red restantes en el dispositivo para supervisar el tráfico de base de datos y no tienen asignada una dirección IP.

Tema principal: Paso 4. Establecer la configuración inicial y básica

Establecer la dirección IP predeterminada del direccionador

Utilice el siguiente mandato de CLI:

```
store network routes defaultroute <ip_direccionador_predeterminada>
```

Tema principal: Paso 4. Establecer la configuración inicial y básica

Establecer la dirección IP del servidor DNS

Establezca la dirección IP de uno o varios servidores DNS que utilizará el dispositivo para resolver los nombres de host y las direcciones IP. Se requiere el primer resolvedor, los otros son opcionales.

```
store network resolver 1 <resolver_1_ip>
store network resolver 2 <resolver_2_ip>
store network resolver 3 <resolver_3_ip>
```

Tema principal: Paso 4. Establecer la configuración inicial y básica

Servidor SMTP

Es necesario un servidor SMTP para enviar alertas del sistema. Especifique los mandatos siguientes para establecer la dirección IP del servidor SMTP, establecer una dirección de retorno para los mensajes y habilitar las alertas SMTP al arrancar.

```
store alerter smtp relay <servidor_smtp>
store alerter smtp returnaddr <first.last@company.com>
store alerter state startup on
```

Nota: También puede configurar el servidor SMTP utilizando la interfaz de usuario. Pulse Configurar > Alertador.
Tema principal: Paso 4. Establecer la configuración inicial y básica

Establecer el nombre de host y el nombre de dominio

Configure el nombre de host y el nombre de dominio del dispositivo. Este nombre debe coincidir con el nombre de host registrado para el dispositivo en el servidor DNS.

```
store system hostname <nombre_host>
store system domain <nombre_dominio>
```

Tema principal: Paso 4. Establecer la configuración inicial y básica

Establecer el huso horario, la fecha y la hora

Hay opciones para establecer la fecha y hora del dispositivo.

Huso horario, fecha, hora y ntp

1. Establecer huso horario
2. Establecer fecha y hora - Opción 1: Establecer ntp. Opción 2 - store system clock datetime

Opción fecha/hora 1: Network Time Protocol

Proporcione los detalles de un servidor NTP accesible y habilite su uso.

```
store system ntp server
store system ntp state on
```

Opción fecha/hora 2: Establecer el huso horario, fecha y hora

Utilice el mandato siguiente para visualizar una lista de husos horarios válidos:

```
store system clock timezone list
```

Elija el huso horario adecuado en la lista y utilice el mismo mandato para establecerlo.

```
store system clock timezone <huso horario seleccionado>
```

Nota: Cuando se configura un nuevo huso horario, los servicios internos se reinicia y se inhabilita la supervisión de datos durante unos minutos durante este reinicio.

Almacene la fecha y hora, con el formato: AAAA-mm-dd hh:mm:ss

```
store system clock datetime <fecha_hora>
```

Nota: No cambie el nombre de host ni el huso horario en la misma sesión de CLI.

Tema principal: Paso 4. Establecer la configuración inicial y básica

Establecer el tipo de unidad inicial

Un dispositivo puede ser una unidad autónoma, un gestor o una unidad gestionada. Además, se puede establecer un dispositivo para capturar la actividad de la base de datos a través de la inspección de red o S-TAP o ambas cosas. La configuración estándar será para un dispositivo autónomo (para todos los dispositivos), y el valor más común utilizará la captura S-TAP (sólo para los recopiladores).

store unit type standalone: Utilice este mandato para todos los dispositivos.

store unit type stap: Utilice este mandato para los recopiladores.

De forma predeterminada, están establecidos el tipo de unidad autónoma y el tipo de unidad stap. El tipo de unidad de gestor se debe especificar, si es necesario.

Nota: Los valores de tipo de unidad se pueden establecer en una fase posterior, cuando el dispositivo esté totalmente operativo.
Tema principal: Paso 4. Establecer la configuración inicial y básica

Restablecer la contraseña root

Restablezca su contraseña root en el dispositivo utilizando su propia passkey privada mediante el siguiente mandato de CLI (requiere la clave de acceso *"t0Tach"*):

```
support reset-password root <random>
```

Guarde la passkey que ha utilizado en su documentación, para permitir el acceso root al servicio de soporte técnico. Para ver la passkey actual, utilice el mandato de CLI siguiente:

```
support show passkey root
```

Preguntas - ¿Qué nivel de seguridad tiene la contraseña root de Guardium? ¿Quién puede acceder a la misma?

Los dispositivos Guardium son entornos de "caja negra" y únicamente los usuarios finales tienen acceso a las cuentas del sistema operativo de acceso limitado, tales como:

cli, guardcli1, guardcli2, guardcli3, guardcli4 y guardcli5.

Las cuentas de usuario de la interfaz gráfica de usuario, por ejemplo admin y accessmgr, no las define el sistema operativo del sistema Guardium, sino que son ID de aplicación definidos y gestionados por una interfaz de aplicación (accessmgr).

Dado que se trata de un servidor protegido, el acceso root no está disponible fácilmente para nadie, normalmente es necesario que el servicio de soporte de Guardium obtenga acceso a los dispositivos de Guardium para la resolución de problemas. El servicio de soporte de Guardium no utiliza sudo, ni ningún otro ID de usuario que no sea root, para acceder a los dispositivos Guardium.

La contraseña root está protegida mediante un mecanismo de "contraseña conjunta". El cliente tiene las claves para el dispositivo con un formato de passkey numérica de ocho dígitos. IBM tiene el codificador de passkey. Sin ambas cosas, la passkey y el decodificador de passkey, ni IBM ni el cliente pueden acceder al dispositivo como root.

La passkey la gestiona el cliente mediante la interfaz de CLI. En cualquier momento, el cliente puede cambiar la passkey sin notificar a IBM, utilizando el siguiente mandato de CLI:

```
support reset-password root
```

Cualquier usuario con acceso de CLI puede recuperar la passkey de usuario root utilizando el siguiente mandato de CLI:

```
support show passkey root
```

Cuando participa el servicio de soporte de Guardium, en una sesión compartida de escritorio remoto, el analista de soporte solicita la passkey de roo para el dispositivo Guardium en cuestión. Una vez decodificada la passkey, el servicio de soporte de Guardium utiliza la contraseña root para acceder al dispositivo como root. Una vez terminada la sesión de escritorio compartido, el cliente puede cambiar la passkey utilizando el mandato de CLI anterior y de este modo se asegura de que IBM ya no tenga la contraseña root para este dispositivo.

Dado que se trata de una clave numérica de ocho dígitos, la clave tiene un rango de 10000000 a 99999999. Este rango proporciona 89.999.999 contraseñas posibles. Todas las contraseñas codificadas están reforzadas. No contienen ninguna contraseña común, ninguna palabra de diccionario, su longitud varía y contienen caracteres nacionales, especiales, alfabéticos (mayúsculas y minúsculas) y/o numéricos.

El acceso al decodificador de passkeys está restringido a un número reducido de empleados de IBM Guardium, tales como Guardium R&D, Guardium QA y los miembros del personal de soporte de Guardium. No está disponible para el personal de IBM.

Los ID de usuario de CLI mencionados anteriormente (cli, guardcli1, guardcli2, guardcli3, guardcli4, guardcli5) no utilizan el mecanismo de passkey y sus contraseñas las rige el cliente al 100%, IBM no tiene acceso a sus contraseñas. Por este motivo, IBM recomienda mantener la passkey de root en un recinto de seguridad de contraseñas para garantizar que se pueda acceder al dispositivo, incluso si las contraseñas de la cuenta de CLI se han olvidado o no se encuentran.

Tema principal: Paso 4. Establecer la configuración inicial y básica

Validar todos los valores

Antes de cerrar sesión en la CLI y pasar al siguiente paso de configuración, revise y valide los valores configurados, utilizando los siguientes mandatos:

```
show network interface all
show network routes defaultroute
show network resolver all
show system hostname
show system domain
show system clock timezone
show system clock datetime
show system ntp all
show unit type
```

Tema principal: Paso 4. Establecer la configuración inicial y básica

Rearrancar el sistema

Si el sistema no está en su ubicación final, ahora es un buen momento para concluir el sistema, colocarlo en su ubicación final de red e iniciarlo de nuevo.

Extraiga el DVD de instalación antes de reiniciar el sistema.

Para detener el sistema, especifique el mandato siguiente en la CLI:

```
stop system
```

El sistema concluye. Traslade el sistema a su ubicación final, vuelva a cablear el sistema y encienda de nuevo el sistema. Después de encender el sistema, se puede acceder al mismo (utilizando la CLI y la GUI) a través de la red, utilizando la dirección IP o el nombre de host proporcionados.

Tema principal: Paso 4. Establecer la configuración inicial y básica

Paso 5. Qué hacer a continuación

Esta sección describe los pasos para verificar la instalación, instalar las claves de licencia e instalar cualquier parche de mantenimiento disponible.

- Verificar si la instalación es correcta
  Verifique la instalación realizando los pasos siguientes:
- Establecer el tipo de unidad
  Para configurar un entorno federado, configure uno de los dispositivos como el gestor central y establezca los otros dispositivos de modo que los gestione el gestor central.
- Instalación de las claves de licencia
  Este tema le guía por los pasos para instalar y aceptar las claves de licencia de Guardium.

- Instalar parches de mantenimiento (si están disponibles)
  Puede instalar parches utilizando la CLI o la GUI.
- Pasos adicionales (opcional)
  En las secciones siguientes se describe cómo cambiar el idioma inglés de línea base a otro idioma, cómo instalar agentes de S-TAP, definiendo los motores de inspección e instalando los agentes de CAS.

Tema principal: Instalación del sistema Guardium

Verificar si la instalación es correcta

Verifique la instalación realizando los pasos siguientes:

1. Inicie sesión en la CLI: ssh cli@<ip de dispositivo>
2. Inicie sesión en la GUI: https://<nombre de host de dispositivo>.<dominio completo>:8443 (utilice el id de usuario admin)

El primer inicio de sesión después del reinicio requiere cambiar las contraseñas.

Inicie sesión en la interfaz de Guardium basada en web y vaya a la ayuda en línea incluida para obtener más información acerca de cualquiera de las tareas siguientes.

Tema principal: Paso 5. Qué hacer a continuación

Establecer el tipo de unidad

Para configurar un entorno federado, configure uno de los dispositivos como el gestor central y establezca los otros dispositivos de modo que los gestione el gestor central.

Utilice el mandato de CLI store unit type para establecer el tipo de cada sistema Guardium.

Tema principal: Paso 5. Qué hacer a continuación

Instalación de las claves de licencia

Este tema le guía por los pasos para instalar y aceptar las claves de licencia de Guardium.

Antes de empezar

- Descargue las claves de licencia en Passport Advantage
- Instale o actualice su sistema Guardium.
- Verifique que el tipo de máquina se ha establecido correctamente para el sistema

Acerca de esta tarea

Instalar una clave de licencia de Guardium es un proceso de dos pasos: Debe instalar la clave de licencia y, a continuación, leer y aceptar los términos del acuerdo de licencia. Después de instalar una clave de licencia Guardium, se vuelve a cargar la interfaz de usuario para mostrar las funciones que ha habilitado la nueva licencia.

Para establecer un sistema Guardium funcional es necesario instalar una licencia base y al menos una licencia de adición. La licencia base debe estar instalada y aceptada antes de instalar y aceptar las licencias de adición.

Para obtener más información sobre las claves de licencia de Guardium, consulte Claves de licencia.

Atención:

Cuando se actualiza un sistema Guardium, no es necesario aplicar las licencias. Las claves de licencia se generan automáticamente en función de la instalación ya existente, pero debe revisar y aceptar los acuerdos de licencia para poder empezar a utilizar el sistema Guardium. Para revisar y aceptar las licencias en un sistema actualizado, vaya a Configuración > Herramientas y vistas > Licenciay pulse el enlace Leer y aceptar.

Procedimiento

1. Inicie sesión en el sistema Guardium como usuario `admin`.
2. Verifique que el Tipo de máquina que se muestra en el banner de Guardium sea correcta para el sistema para el que adquiere la licencia. El tipo de máquina será uno de los siguientes:
   - Autónomo
   - Gestor central
   - Agregador

   Atención: Si configura un gestor central y el Tipo de máquina indica un agregador, convierta el sistema de agregador a gestor central, utilizando el siguiente mandato de CLI: `store unit type manager`.
3. Instale una licencia base.
   a. Vaya a Configurar > Herramientas y vistas > Licencia.
   b. En la página Licencia, especifique la clave base para el sistema en el campo Clave de licencia y pulse Aplicar para continuar.
   Atención: En función del sistema que esté configurando, tendrá que aplicar una clave de recopilador base o una clave de agregador base. Se requiere una clave de agregador base cuando se configura un sistema de gestor central.
   c. En el diálogo Acuerdo de licencia, revise el acuerdo de licencia asociado con la clave base y pulse Aceptar cuando esté listo para aceptar los términos. La interfaz de Guardium se renueva automáticamente una vez aceptado el acuerdo, pero no habrá ningún cambio en las funciones disponibles después de instalar una clave de licencia base.
4. Instale una o varias licencias de adición. Repita los pasos siguientes para cada licencia de adición que haya adquirido y desee instalar.
   a. Vaya a Configurar > Herramientas y vistas > Licencia.
   b. En la página Licencia, especifique la clave de adición en el campo Clave de licencia y pulse Aplicar para continuar.
   c. En el diálogo Acuerdo de licencia, revise el acuerdo de licencia asociado con la clave de adición y pulse Aceptar cuando esté listo para aceptar los términos. La interfaz de Guardium se renueva automáticamente una vez aceptado el acuerdo, y cualquier función nueva asociada a la licencia de adición pasará a estar disponible.

d. Repita los pasos de esta sección para cada licencia de adición que desee instalar.

Qué hacer a continuación

En un entorno con un gestor central, puede distribuir las nuevas licencias desde la página Gestionar > Gestión central > Gestión central y pulsando el icono para distribuir las licencias desde el gestor central a las unidades gestionadas.

En un entorno con un gestor central, el gestor central y sus unidades gestionadas deben utilizar el mismo secreto compartido. Establezca el secreto compartido en la página Configuración > Herramientas y vistas > Sistema o utilizando el mandato de CLI store system shared secret.

Tema principal: Paso 5. Qué hacer a continuación
Conceptos relacionados:
Claves de licencia

Instalar parches de mantenimiento (si están disponibles)

Puede instalar parches utilizando la CLI o la GUI.

Nota: En entornos federados, los parches de mantenimiento se pueden aplicar a todos los dispositivos desde el gestor central.

Es posible que no haya ningún parche de mantenimiento incluido con los materiales de instalación. Si se incluye alguno, siga estos pasos para aplicarlos:

1. Inicie sesión en la consola de Guardium como usuario cli, utilizando la contraseña cli temporal que ha definido en el procedimiento de instalación anterior. Puede hacerlo utilizando un cliente ssh.
2. Realice una de las acciones siguientes:
   - Si realiza la instalación desde una ubicación de red, especifique el mandato siguiente (seleccionando ftp o scp):

     ```
     store system patch install [ftp | scp]
     ```

     Y responda a las solicitudes siguientes (asegúrese de proporcionar el nombre completo de la vía de acceso del archivo de parche):

     Host desde el que importar el parche:

     Usuario en <hostname>

     Vía de acceso completa al parche, incluido el nombre:

     Contraseña:

   - Si está realizando la instalación utilizando la función fileserver, entre el mandato siguiente:

     ```
     store system install patch sys
     ```

     Se le solicitará que seleccione el parche que desea aplicar. Utilice comodines en el nombre de vía de acceso para obtener varios parches. Separe los nombres de parches con comas.
3. Para instalar parches adicionales, repita el paso 2.
4. Para ver si se han instalado correctamente los parches, utilice el mandato de CLI:

   ```
   show system patch installed
   ```

   Los parches se instalan mediante un proceso en segundo plano que puede tardar unos minutos en completarse.

Tema principal: Paso 5. Qué hacer a continuación

Pasos adicionales (opcional)

En las secciones siguientes se describe cómo cambiar el idioma inglés de línea base a otro idioma, cómo instalar agentes de S-TAP, definiendo los motores de inspección e instalando los agentes de CAS.

Cambiar el idioma

La instalación de IBM Guardium siempre está en inglés. Utilice el mandato de CLI store language para cambiar el inglés de línea base y convertir la base de datos al idioma preferido. Un sistema Guardium sólo se puede cambiar a japonés o chino (tradicional o simplificado) después de una instalación. El mandato store language se considera una configuración del sistema Guardium y está previsto que se ejecute durante la configuración inicial del sistema. La ejecución de este mandato de CLI después del despliegue del dispositivo en un idioma específico puede cambiar la información ya capturada, almacenada, personalizada, archivada o exportada. Por ejemplo, los psmls (los paneles y portlets que ha creado) se suprimirán, ya que es necesario volver a crearlos en el nuevo idioma.

Nota: Para evitar que la IU de Guardium muestre una combinación de idiomas, establezca el gestor central y las unidades gestionadas en el mismo idioma.

Instalar agentes de S-TAP

Instale los agentes de S-TAP en los servidores de bases de datos y defina sus motores de inspección. S-TAP es un agente de software ligero instalado en el servidor de bases de datos, que supervisa el tráfico de base de datos local y de red y envía la información relevante a un sistema Guardium (el recopilador) para realizar tareas adicionales de análisis, generación de informes y alertas. Para instalar un S-TAP, consulte la sección S-TAP de este Information Center. Para verificar que los S-TAP se han instalado y están conectados al sistema Guardium:

1. Inicie sesión en el portal del administrador.
2. Realice una de las acciones siguientes:

Vaya a Gestionar > Vista de sistema y pulse Supervisor de estado de S-TAP en el menú. Se muestran todos los S-TAP con un fondo verde. Un fondo rojo indica que el S-TAP no está activo.

Vaya a Gestionar > Supervisión de actividad > Control de S-TAP confirme que este S-TAP tiene una luz verde.

Definir motores de inspección

Defina los motores de inspección para la supervisión de actividades basada en red.

Instalar agentes CAS

Instale los agentes CAS (Configuration Auditing System) en el servidor de base de datos.

Tema principal: Paso 5. Qué hacer a continuación

Crear la imagen virtual

Utilice esta sección para instalar la imagen virtual.

- Visión general de la infraestructura de VMware
  Aunque puede instalar una MV de Guardium en cualquier producto de VMware, el servidor VMware ESX es la plataforma recomendada para una solución virtual y se presenta aquí.
- Visión general de la instalación de la MV
  Siga estos pasos para instalar la MV de IBM Security Guardium. Después de instalar la MV, vuelva al paso 3 anterior, instale la imagen de IBM Security Guardium y vaya al Paso 4 anterior, de Configuración inicial y configuración básica.
- Creación de una máquina virtual de Hyper-V

Tema principal: Instalación del sistema Guardium

Visión general de la infraestructura de VMware

Aunque puede instalar una MV de Guardium en cualquier producto de VMware, el servidor VMware ESX es la plataforma recomendada para una solución virtual y se presenta aquí.

El servidor VMware ESX en el que puede instalar la MV de Guardium es un componente de la infraestructura de VMware. Aunque no todos los componentes de VMware son necesarios para dar soporte a la MV de Guardium, debe estar familiarizado con todos los componentes que se están utilizando en la instalación.

Servidor ESX: Este componente se utiliza para configurar y controlar las máquinas virtuales VMware en un host físico al que se hace referencia como el host del servidor ESX. Para instalar una máquina virtual de Guardium, en primer lugar, defina una máquina virtual en un host de servidor ESX y, a continuación, instale y configure la imagen de MV de Guardium en dicha máquina virtual. Puede crear varias MV de Guardium en un único servidor ESX.

Cliente VI (Virtual Infrastructure Client): Este componente se utiliza para conectar con un servidor ESX o con un servidor VirtualCenter. En este último caso, puede administrar varias máquinas virtuales creadas en varios hosts de servidor ESX.

Navegador web: Utilice un navegador web para descargar y utilizar el software del cliente VI desde un host de servidor ESX o desde el servidor de VirtualCenter.

Servidor de gestión de VirtualCenter (Opcional): Este componente se ejecuta en una máquina Windows remota y se puede utilizar para gestionar varias máquinas virtuales en varios hosts de servidor ESX. Ofrece un único punto de control para todos los hosts del servidor ESX.

Base de datos (opcional): El servidor VirtualCenter utiliza una base de datos para almacenar la información de configuración para la infraestructura. La base de datos no es necesaria si no se utiliza el servidor VirtualCenter.

Servidor de licencias (Opcional): Almacena y gestiona las licencias necesarias para mantener una infraestructura de VMware.

Para obtener más información, vaya a www.vmware.com y busque "Inicio rápido de ESX"

Tema principal: Crear la imagen virtual

Visión general de la instalación de la MV

Siga estos pasos para instalar la MV de IBM Security Guardium. Después de instalar la MV, vuelva al paso 3 anterior, instale la imagen de IBM Security Guardium y vaya al Paso 4 anterior, de Configuración inicial y configuración básica.

Si está instalando varios sistemas de MV de Guardium en un entorno de servidor de gestión de VMware VirtualCenter, puede crear un sistema de plantilla a partir de la primera MV de Guardium que crea y, a continuación, clonar esa plantilla según sea necesario. A continuación, todo lo que tiene que hacer es establecer la dirección IP en cada sistema clonado. Para obtener más información, consulte la nota que sigue al Paso 7.

Paso 1: Verificar la compatibilidad del sistema

1. Verifique que el host es compatible con el servidor ESX de VMware (ESX 4.0 actualización 4 y superior es el mínimo necesario para ejecutar un sistema Guardium). En la documentación de VMware, consulte la guía de compatibilidad de sistemas con titularidad para el servidor ESX que está disponible en línea en formato PDF.
2. Verifique que una máquina virtual instalada en el host pueda proporcionar los recursos mínimos recomendados para un sistema Guardium , tanto si tiene previsto utilizarlo como un recopilador, gestor central o agregador. Consulte los recursos mínimos o recomendados en la sección de requisitos de hardware de este documento.
3. Cuando crea una MV de 64 bits por primera vez o actualiza una MV de 32 bits a 64 bits, asegúrese de que el hardware virtual está configurado correctamente para el funcionamiento de 64 bits. En algunos casos, es posible que tenga que realizar una operación de actualización de hardware virtual. Para obtener más información, consulte la documentación de VMware.

Paso 2: Instalar VMware ESX Server

Si todavía no está instalado, instale VMware ESX Server. VMware proporciona instrucciones de instalación en su sitio web para ayudarle a instalar y configurar el servidor ESX y la infraestructura de VMware.

Nota: El servidor ESX solo está soportado en un conjunto específico de dispositivos de hardware. Para obtener más información, consulte la documentación de VMware Virtual Infrastructure.

Paso 3: Conectar cables de red

Antes de definir cualquier conmutador virtual que se vaya a utilizar para la máquina virtual de Guardium, debe conectar las NIC a la red. No puede asignar las NIC a conmutadores o redes virtuales hasta que las NIC estén conectadas físicamente.

En la tabla siguiente se describe cómo la MV de Guardium utiliza las interfaces de red. Consulte esta tabla para realizar las conexiones adecuadas antes de configurar los conmutadores virtuales para que los utilice la MV de Guardium.

Tabla 1. Uso de la interfaz de red de MV de IBM Security Guardium

Interfaz	Descripción
Interfaz proxy (eth0)	Esta interfaz es la pasarela principal para el dispositivo y se utiliza para estos fines: • Interfaz gráfica de usuario (GUI) basada en web para gestionar, configurar y utilizar la solución • Interfaz de línea de mandatos (CLI) para la configuración inicial y la configuración básica • Las conexiones con sistemas externos, tales como los sistemas de copia de seguridad, servidores de base de datos y el servidor LDAP • La comunicación con otros componentes de Guardium, tales como dispositivos (agregador, gestor central) y agentes instalados en los servidores de bases de datos o de archivos, tales como clientes CAS o S-TAP.
Interfaz del servidor de aplicaciones (eth1)	Esta interfaz es necesaria si configura el sistema Guardium como un proxy transparente. Se conecta a los servidores de aplicaciones cuyo contenido se ha configurado para que lo enmascare Guardium.

Paso 4: Configurar el portal de gestión de la MV de Guardium

La configuración predeterminada de una nueva instalación de VMware ESX Server crea un único grupo de puertos para que lo utilice la consola de servicio VMware y todas las máquinas virtuales. Para la MV de Guardium, se le recomienda que no comparta puertos con la consola de VMware o con cualquier máquina virtual. Siga estas instrucciones para crear uno o varios conmutadores virtuales para que los utilice una MV de Guardium.

1. Abra el cliente de VMware VI e inicie sesión en un servidor VirtualCenter o en el host del servidor ESX en el que desee crear una nueva máquina virtual.
2. Si ha iniciado la sesión en un servidor VirtualCenter, pulse Inventario en la barra de navegación y expanda el inventario, según sea necesario, para visualizar el host o clúster gestionado en el que tiene previsto instalar una MV de Guardium.
3. En la pantalla de inventario, pulse el host o clúster en el que tiene previsto instalar una MV de Guardium.
4. Pulse el separador Configuración, pulse Redes en el recuadro Hardware y luego pulse Añadir red.

Esto abre el asistente Añadir red, que se utiliza para varios fines.

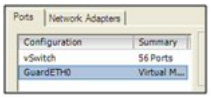
Utilice el asistente Añadir red para definir un nuevo conmutador virtual para la interfaz de red de la MV de Guardium. Esta es la conexión mediante la que accederá a la consola de gestión de la MV de Guardium y mediante la cual la máquina virtual de Guardium se comunicará con otros componentes de Guardium (S-TAP, por ejemplo, que son agentes de software que instalará posteriormente en uno o más servidores de bases de datos).

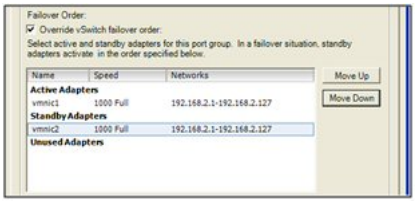
5. En el recuadro Tipos de conexión, pulse Máquina virtual y pulse Siguiente.
6. En el panel Acceso de red, pulse Crear un conmutador virtual y marque el adaptador de red no reclamado que utilizará para la interfaz de red la MV de Guardium :

7. Opcionalmente, marque un segundo adaptador de red no reclamado si desea utilizar la función de agrupación de las IP de VMware para proporcionar una interfaz de red secundaria (migración tras error). Posteriormente, designará este segundo adaptador como un adaptador en espera (y, por supuesto, debe cablear ambas NIC de la forma adecuada).
8. Pulse Siguiente para continuar en la página Valores de conexión del asistente Añadir red.
9. En el recuadro Etiqueta de red, especifique un nombre para el grupo de puertos de la máquina virtual, por ejemplo: GuardETH0, y pulse Siguiente.

10. En la página Resumen, pulse Finalizar. El nuevo conmutador virtual se visualiza en el separador Configuración.
11. Opcional. Si ha definido un segundo adaptador con fines de migración tras error: (a) Pulse Enlace de propiedades para el conmutador virtual que acaba de crear para abrir el panel de propiedades del conmutador virtual. (b) Pulse el separador Puertos y seleccione el grupo de puertos virtuales que acaba de crear (GuardETH0 en el ejemplo), y pulse Editar. (c) En el panel Propiedades del grupo de puertos virtuales, pulse el separador Agrupación de NIC, marque el recuadro Alterar

temporalmente la migración tras error de vSwitch y, a continuación, mueva el segundo adaptador a la lista de adaptadores en espera. (d) Pulse Aceptar para cerrar el recuadro de propiedades del grupo de puertos virtuales y pulse Cerrar para cerrar el recuadro de propiedades del conmutador virtual.





Paso 5: Crear una nueva máquina virtual

Si todavía no lo ha hecho, cree una nueva máquina virtual en la que instalará una MV de Guardium.

Realice esta tarea utilizando el cliente VI de VMware.

1. Abra el cliente de VMware VI e inicie sesión en un servidor VirtualCenter o en el host del servidor ESX en el que desee crear una nueva máquina virtual.
2. Si ha iniciado sesión en un servidor VirtualCenter, pulse Inventario en la barra de navegación y expanda el inventario, según sea necesario, para visualizar el host o clúster gestionado en el que tiene previsto instalar la nueva máquina virtual.
3. En el menú Archivo, pulse Nueva - Máquina virtual para el panel de tipo de configuración del asistente de Nueva máquina virtual.
4. Pulse Típica como el tipo de configuración y pulse Siguiente para continuar en el panel Nombre y carpeta.
5. En el panel Nombre y carpeta:

   Escriba un nombre para la nueva máquina virtual en el campo Nombre de máquina virtual. Este nombre aparece en el inventario del cliente VI y también se utiliza como el nombre de los archivos de las máquinas virtuales.

   Para establecer la ubicación de inventario para la nueva máquina virtual, seleccione una carpeta o la ubicación raíz de un centro de datos en la lista situada debajo de Ubicación de inventario de máquina virtual.

   Pulse Siguiente.

6. Si el host o el clúster contiene agrupaciones de recursos, se muestra el panel Agrupación de recursos y debe seleccionar el recurso (host, clúster o agrupación de recursos) en el que desea ejecutar la máquina virtual. Pulse Siguiente.
7. En panel de almacén de datos, opcionalmente seleccione un almacén de datos para almacenar los nuevos archivos de máquina virtual y pulse Siguiente.
8. En el panel Seleccionar el sistema operativo invitado, seleccione el sistema operativo correspondiente a la imagen de Guardium que está instalando. Pulse Linux > RedHat Enterprise Linux 6, 64 bits en el recuadro Versión y pulse Siguiente. .

   El sistema operativo no se instala ahora, pero el tipo de SO es necesario para establecer los valores predeterminados para la máquina virtual.

   Para obtener información acerca de los recursos mínimos de la MV, consulte el apartado de requisitos de hardware en la sección Antes de empezar.

9. En el panel de CPU virtuales, seleccione el número de CPU recomendadas para el tipo de MV de Guardium que se va a instalar y pulse Siguiente.
10. En el panel Memoria, seleccione la cantidad de memoria recomendada para el tipo de MV de Guardium que está instalado y pulse Siguiente. Importante: El valor inicial debe ser como mínimo de 16 GB. Si los clientes desean trabajar fuera del rango necesario, póngase en contacto con el servicio de soporte técnico.
11. En el panel Red, pulse 1 como el número de puertos necesarios y pulse Siguiente.
12. Para el puerto seleccionado, utilice el menú desplegable Red para elegir un grupo de puertos configurado para que lo utilice la red virtual. (Debe haber definido este grupo de puertos en el procedimiento anterior).
13. Para el grupo de puertos seleccionados, seleccione el recuadro de selección Conectar al encender, (debe estar marcado de forma predeterminada), y pulse Siguiente.
14. En el panel Capacidad de disco virtual, especifique la cantidad de espacio de disco que se debe reservar para la nueva máquina virtual en el campo Tamaño de disco.
15. En el panel Listo para completarse, verifique los valores y pulse Finalizar.

Esta tarea completa la definición de la nueva máquina virtual. El sistema operativo todavía no se ha instalado, por lo que si intenta iniciar la máquina virtual, esta actividad fallará.

Paso 6: Instalar el sistema Guardium

Realice esta tarea utilizando el cliente de VMware Virtual Infrastructure.

1. Abra el cliente de VMware VI e inicie sesión en un servidor VirtualCenter o en el host del servidor ESX en el que desee crear una nueva máquina virtual.
2. Si ha iniciado sesión en un servidor VirtualCenter, pulse Inventario en la barra de navegación, expanda el inventario, según sea necesario, y seleccione la máquina virtual en la que desea instalar la MV de Guardium.
3. En el separador Resumen, pulse Editar valores.
4. Pulse Unidad 1 de CD/DVD.
5. Seleccione una de las opciones siguientes para determinar a partir de qué ubicación el dispositivo de CD-ROM/DVD virtual leerá el programa de instalación de Guardium. **Le recomendamos encarecidamente la primera opción**:

   Archivo ISO de almacén de datos - Conéctese al archivo ISO de instalación de Guardium en un almacén de datos. Si todavía no lo ha hecho, copie los archivos ISO de Guardium en un almacén de datos accesible desde el host del servidor ESX en el que está instalada la máquina virtual. Pulse Examinar para seleccionar el archivo.

   Atención: En las opciones restantes, instará el CD/DVD de instalación de Guardium en una unidad de CD-ROM/DVD. Si reinicia cualquier sistema con un CD/DVD de instalación de Guardium insertado en su unidad de CD-ROM/DVD, instalará Guardium y borrará el sistema operativo del host y los archivos.

Dispositivo de cliente - Conecte con un dispositivo de CD-ROM/DVD en el sistema en el que está ejecutando el cliente VI. Si selecciona esta opción, inserte el CD/DVD de Guardium en la unidad de CD-ROM/DVD del sistema en el que se ejecuta el cliente VI.

Dispositivo de host - Conéctese a un dispositivo de CD-ROM/DVD en la máquina host del servidor ESX en la que está instalada la máquina virtual. Si selecciona esta opción, elija el dispositivo en el menú desplegable e inserte el CD/DVD de Guardium en la unidad de CD-ROM/DVD de la máquina host del servidor ESX.

6. Pulse Aceptar.
7. Pulse Encendido para iniciar la máquina virtual.
8. Si ha selección el dispositivo de cliente como su opción de unidad de CD/DVD, pulse CD-ROM virtual (ide0:0) en la barra de herramientas y seleccione el dispositivo de CD-ROM local al que se ha de conectar.
9. Pulse el separador Consola para visualizar la consola de la máquina virtual. Tendrá que responder a varias solicitudes durante el proceso de instalación.
10. Omita este paso si está utilizando el DVD de Guardium.

    Cuando se le solicite el segundo CD, en función de la opción que utilice en el paso 5, deberá insertar el segundo CD en su unidad o seleccionar la imagen ISO del segundo CD. Continúe pulsando Intro. Cuando se le solicite la contraseña cli, especifique una contraseña temporal para utilizarla al iniciar sesión en la CLI de Guardium, Lo cual es necesario para establecer los parámetros de configuración de IP para el dispositivo.

11. Cuando se le solicite la contraseña de administración de la GUI, especifique una contraseña temporal para utilizarla al iniciar la sesión en la interfaz de usuario de Guardium como usuario administrador.
12. Cuando se le pregunte si está creando un recopilador o un agregador, elija el tipo adecuado.
13. Haga clic en No en la solicitud de Passkey maestra.

    Atención: Si se ha utilizado una unidad de CD-ROM/DVD, se expulsa el CD/DVD cuando finaliza la instalación. Asegúrese de que extrae el CD/DVD de instalación de dicha unidad. Si se ha utilizado el archivo ISO, asegúrese de extraer el CD ROM de ISO, volviendo a cambiar el CD/DVD virtual al dispositivo de cliente o host. De lo contrario, la próxima vez que se reinicie, instalará Guardium en la máquina host borrará el sistema operativo de la máquina de host y todos los archivos.

    La máquina se reiniciará automáticamente y se le solicitará que inicie sesión como usuario de CLI.

14. Llegado a este punto, regrese al Paso 4, Configuración inicial y configuraciones básicas, para completar las instrucciones de configuración del sistema Guardium.

Paso 7: Instalar varias MV

(Opcional) Para instalar varias MV de Guardium, puede repetir los procedimientos para cada dispositivo o puede minimizar el trabajo clonado la primera MV de Guardium que ha creado y siguiendo estos pasos:

1. Utilice el producto de servidor de VMware Virtual Infrastructure para clonar la primera MV de Guardium que ha configurado en una plantilla.
2. En la plantilla, cree un clon para cada MV de Guardium adicional que se ha de configurar.
3. Para cada clon, inicie sesión en la consola de la MV de Guardium como usuario cli, utilizando la contraseña cli temporal y restablezca cualquiera de los parámetros de configuración de IP que ha establecido en el procedimiento anterior. Las tareas obligatorias son: Restablecer la dirección IP y restablecer el nombre de host (store system hostname). No obstante, revise todos los valores de configuración de IP especificados en el procedimiento anterior.

   ```
   store network interface ip <dirección_ip>
   store network interface mask <máscara_subred>
   store system hostname <nombre_host>
   ```

   Cuando haya terminado, escriba el mandato restart network.

   ```
   restart network
   ```

   Nota: El ID exclusivo del dispositivo se vuelve a calcular cada vez que se cambia el nombre de host, para evitar que muchos dispositivos tengan el mismo ID exclusivo.

Tema principal: Crear la imagen virtual

Creación de una máquina virtual de Hyper-V

Antes de empezar

- Hyper-V es una solución de virtualización de Microsoft. Se presupone que el usuario de Guardium que utiliza Hyper-V tiene experiencia previa con Hyper-V. La mayoría de las instalaciones de Hyper-V son directas. Las instrucciones que se listan en este tema de ayuda de Guardium pueden ser más complejas de lo necesario.
- Verifique los requisitos del sistema para la versión de Guardium que se está instalando.
- Reserve una dirección IP para la máquina virtual.

Acerca de esta tarea

Procedimiento

1. Inicie sesión en el servidor de Hyper-V como administrador.
2. Inicie el gestor de Hyper-V en el menú Inicio > Herramientas administrativas > Gestor de Hyper-V.
3. Pulse con el botón derecho el servidor de Hyper-V y seleccione Nuevo > Máquina virtual.
   a. Especifique el nombre de host en el campo Nombre, utilice la ubicación predeterminada Almacén y, a continuación, pulse Siguiente.
   b. Especifique la memoria deseada en el campo RAM y, a continuación, pulse Siguiente. Verifique que la RAM especificada cumpla los requisitos mínimos del sistema para su versión de Guardium.
   a. Seleccione Conexión troncal > Red virtualy, a continuación, pulse Siguiente.
   b. Especifique el tamaño de disco deseado en el diálogo Disco virtual y pulse Siguiente. Verifique que el disco virtual especificado cumpla los requisitos mínimos del sistema para su versión de Guardium.
   c. Acepte los valores predeterminados en Opciones de instalación y, a continuación, pulse Siguiente.
   d. Pulse Finalizar para crear la nueva máquina virtual.
4. Pulse con el botón derecho la nueva máquina virtual en la lista Máquinas virtuales y seleccione Conectar para abrir la consola.
5. Encienda la máquina virtual para reservar una dirección MAC pulsando el botón verde o seleccionando Acción > Iniciar.
6. En el indicador de error de arranque, apague la máquina virtual pulsando el botón gris o seleccionando Acción > Apagar.

7. Seleccione Archivo > Valores para continuar configurando la máquina virtual.
    a. Especifique el número deseado de procesadores lógicos en Hardware > Procesador > Procesadores lógicos. Verifique que número de procesadores especificado cumpla los requisitos mínimos del sistema para su versión de Guardium.
    b. Anote la dirección MAC asignada en Hardware > Adaptador de red. Necesitará esta información más adelante en el proceso de instalación.
    c. Seleccione el adaptador de red y pulse Eliminar.
    d. Seleccione Hardware > Añadir hardware > Adaptador de red existente y pulse Añadir. La selección se mueve automáticamente a Adaptador de red existente.
    e. Seleccione Conexión troncal > Red virtual.
    f. Seleccione Dirección MAC > Estática y especifique la dirección MAC registrada anteriormente.
    g. Seleccione el recuadro de selección Habilitar identificación de LAN virtual.
    h. Escriba una Designación de VLAN de `3xxx`. Por ejemplo, `3156`.
    i. Seleccione Hardware > BIOS, suba el Adaptador de red existente y pulse Aceptar.
8. Añada la dirección MAC de la máquina virtual a su reserva de IP.
9. Añada la dirección IP, el nombre de host y la dirección MAC de la máquina virtual a gmachine_list.txt.
10. Inicie la máquina virtual. Cuando se muestre el diálogo Arranque de SO de Dev-IT, deténgase en BOOT: hasta que se exceda el tiempo de espera y regrese a la solicitud Error de arranque.
11. Ejecute el mandato PXE y, a continuación, utilice el botón de macro Ctrl-Alt-Supr para rearrancar la máquina virtual. Permita que la máquina se compile.
12. Utilice TOUCH y SU-CLI para asignar los valores de dirección IP, ruta y DNS adecuados. Normalmente, los valores de host y dominio se configuran automáticamente.
13. Utilice SU - CLI > STOP SYSTEM para concluir el sistema.
14. Pulse con el botón derecho la máquina virtual y seleccione Valores.
    a. Sustituya el Adaptador de red existente por la selección de adaptador de red predeterminado.
    b. Seleccione Conexión troncal > Red virtual.
    c. Seleccione Dirección MAC > Estática y especifique la dirección MAC registrada anteriormente.
    d. Escriba una Designación de VLAN de `3xxx`. Por ejemplo, `3156`.
15. Inicie la máquina virtual.

Qué hacer a continuación

Verifique que la máquina virtual esté en funcionamiento haciendo ping a OTIS desde la máquina virtual e inicie sesión en la máquina virtual mediante SSH desde un host remoto.

Estos son problemas comunes:

- Si no se sustituye el adaptador de red predeterminado por el adaptador existente, no se permite el acceso a PXE.
- Si no se sustituye el adaptador de red existente por el adaptador predeterminado, deje el sistema Guardium sin conectividad de red.
- Si después de sustituir el adaptador de red existente, se inicia la máquina antes de cambiar la dirección MAC, se genera una nueva dirección MAC y un nuevo adaptador virtual en la máquina virtual. Esto se debe solucionar para que funcione el sistema. Cambie la dirección MAC por la dirección MAC registrada anteriormente y utilice el método normal para borrar ifcfg-eth0 y 70-persistent-nework.rules.

Tema principal: Crear la imagen virtual

Particionamiento personalizado

Si personaliza el particionamiento de la unidad de disco duro, debe realizar varias elecciones.

1. Elija la instalación de partición personalizada en la pantalla de arranque.
   Elija Crear diseño personalizado y utilice el esquema de particionamiento recomendado que se describe aquí.
   Nota: El gestor de arranque, un programa especial que carga el sistema operativo en la memoria, forma parte de cualquier instalación de particionamiento personalizada.
2. Crear un diseño personalizado. En este caso, hay particiones existentes en el disco. No suprima ninguna partición. Seleccione el diseño personalizado para añadir las particiones que desee a lo que ya existe en el disco. La tabla siguiente describe los valores recomendados para el diseño personalizado.

Tabla 1. Valores recomendados para el diseño personalizado

Particiones	Valores
/	25 GB
Porción de intercambio	La mitad del tamaño de RAM
/boot	5 GB
/var	Todo lo restante

Todas las unidades disponibles también se visualizan en esta pantalla. Seleccione la unidad para el particionamiento y, a continuación, la instalación.

Una vez finalizado el particionamiento, el software del sistema Guardium se instala automáticamente.

Si se han creado valores que superan el espacio de disco disponible, se muestra un mensaje de error.

Pulse Aceptar para rearrancar el sistema y volver al principio del particionamiento personalizado.

Consulte la documentación de Red Hat Enterprise Linux para obtener más información sobre cómo la distribución de Red Hat maneja el particionamiento.

Tema principal: Instalación del sistema Guardium

Cómo realizar una partición con un LVM cifrado

Si desea utilizar un disco cifrado, siga estos pasos para crear un volumen LVM cifrado que contenga los volúmenes lógicos / y /var.

Para la instalación de LVM cifrado, se le solicitará que especifique una clave de cifrado. A continuación, en CADA rearranque, se solicita al usuario que especifique esta clave para desbloquear el volumen LVM. Esto significa que el usuario debe tener acceso de consola para el dispositivo, ya sea acceso físico o remoto.

Importante: La clave de cifrado debe estar protegida y debe conservarse, ya que no es posible sustituirla si se pierde.

Nota: El gestor de arranque, un programa especial que carga el sistema operativo en la memoria, forma parte de una instalación de particionamiento personalizada. Puede encontrar un ejemplo de la pantalla de entrada de contraseña al final de este tema.

1. Inserte el DVD de IBM Guardium y arranque la máquina.
2. Elija la instalación de partición personalizada en la pantalla de arranque.
3. Pulse Intro.
4. Pulse Eliminar todas las particiones y crear diseño predeterminado en la primera pantalla de RedHat Enterprise Linux. Asimismo, seleccione los recuadros de selección Cifrar sistema y Revisar y modificar diseño de partición.
5. Pulse Siguiente.
6. Se muestra un aviso en la pantalla siguiente en el que se le pregunta si realmente desea eliminar todas las particiones. Pulse Sí.
7. Pulse LogVol00 en la pantalla siguiente y pulse Editar para abrir el diálogo Editar grupo de volúmenes LVM.
8. Pulse LogVol00 en la lista de la pantalla anterior y pulse Editar.
9. En la siguiente pantalla, cambie el tamaño a 10240 y pulse Aceptar.
10. Pulse LogVol01 en la lista de la pantalla siguiente y pulse Editar.
11. Asigne una partición de intercambio cuyo tamaño se la mitad de la memoria instalada en el sistema. Especifique el tamaño de la partición de intercambio y pulse Aceptar.
12. Pulse Añadir. Se muestra el diálogo Crear volumen lógico.
13. Especifique /var como el punto de montaje y deje que el sistema seleccione el tamaño restante.
14. Revise los tamaños de las particiones. A continuación, pulse Aceptar.
15. A continuación, pulse Aceptar en el diálogo Editar grupo de volúmenes LVM: VolGroup00.
16. Pulse Siguiente en la pantalla siguiente, que le llevará al diálogo de frase de contraseña.
17. Escriba la frase de contraseña de su elección en el campo Escribir frase de contraseña y escriba la frase de contraseña idéntica en el campo Confirmar frase de contraseña. Pulse Aceptar.
    Nota: La frase de contraseña se debe especificar cada vez que se arranca el sistema. No hay forma de recuperar una frase de contraseña de LVM perdida.

    Se muestra el diálogo de configuración de bootloader. Cuando se enciende un sistema con Red Hat Enterprise Linux, un programa especial denominado bootloader carga el sistema operativo en la memoria. Normalmente, existe un programa bootloader en el disco duro primario del sistema (o en otro dispositivo de soporte) y su única responsabilidad es cargar el kernel Linux con los archivos necesarios o, en algunos casos, otros sistemas operativos en la memoria.

    En la mayoría de los casos, las opciones predeterminadas son aceptables, pero dependiendo de la situación, es posible que sea necesario cambiar las opciones.

18. En esta pantalla, pulse Siguiente. Esto inicia la instalación cifrada.

    Durante la instalación y rearranques posteriores, se le solicitará que especifique la frase de contraseña LUKS (Linux Unified Key Setup) para el LVM durante el arranque. Después de entrar la frase de contraseña de LUKS, el sistema completa el proceso de arranque.

Tema principal: Instalación del sistema Guardium

Ejemplo de configuración de SAN

Este apéndice describe los pasos necesarios para pasar a un indicador de mandatos para realizar una partición previa de una unidad de disco duro (como es necesario para la instalación de SAN).

En primer lugar, particione el espacio en el dispositivo de almacenamiento SAN y, a continuación, instale el SO de IBM Security Guardium. Elija un disco duro para esta instalación.

Nota: En función del hardware de SAN que se utilice, las instrucciones específicas pueden ser distintas. Se da soporte a la instalación en SAN. La instalación en NAS no está soportada.

Resumen de pasos

1. Entre la configuración del sistema (pulse F1 en los servidores de IBM® durante el arranque inicial) y modifique las Opciones de inicio para seleccionar la ranura PCI para el arranque (donde está la tarjeta QLogic).
2. Modifique el BIOS para la tarjeta QLogic pulsando Ctrl-Q, cuando se esté cargando el BIOS de QLogic, para habilitarlo de modo que sea un dispositivo de arranque. A continuación seleccione el número de unidad lógica (LUN) del dispositivo de arranque.
3. Arranque desde el DVD RedHat 5.8 y entre en modalidad de rescate para ejecutar fdisk y crear particiones en el dispositivo SAN utilizando las especificaciones listadas aquí:

   Tabla 1. Particiones en el dispositivo SAN

Particiones	Espacio
1	500 MB para /boot
2	Cantidad de memoria del sistema + 4 GB
3	25 GB para /
4	Todo el espacio restante para /var

   Nota: Aunque el proceso de instalación de RedHat le permite crear las particiones y cargar el SO, el sistema no arranca correctamente después de la instalación, a menos que las particiones se hayan creado previamente con fdisk.
4. Continúe con la instalación del SO utilizando las particiones definidas anteriormente (utilice solo el dispositivo /dev/sda).
5. Rearranque y finalice los pasos de instalación restantes (nombre de host, configuración IP, etc).

Nota:

En el entorno de SAN, el único LUN se presenta a RedHat 5.8 como varios dispositivos, debido a las vías de acceso redundantes en los conmutadores de red de SAN. (El almacenamiento de SDD era de ocho dispositivos).

Esta es una función de la marca/tipo de almacenamiento de SAN y cómo se configura en cada sitio.

Es muy importante editar únicamente las particiones existentes que ve la instalación de IBM Guardium, añadiendo el punto de montaje y estableciendo el sistema de archivos (ext4 o swap), sin cambiar otros valores (como el tamaño) y deseleccionar todos los dispositivos que no sean /dev/sda cuando se seleccione el dispositivo en que se debe cargar el SO.

Instrucciones para ejecutar fdisk

Siga estas instrucciones para ejecutar fdisk para preparticionar el almacenamiento SAN desde la modalidad de rescate de RedHat:

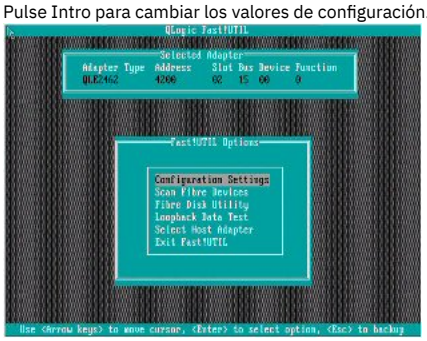
1. Presuponiendo que SAN es el único almacenamiento conectado al servidor, escriba `fdisk /dev/sda`. Escriba `y` si aparece un aviso relacionado con el trabajo en todo el dispositivo.
2. Escriba `n` para una nueva partición.
3. Escriba `p` para una partición primaria.
4. Escriba `1` para la partición #1.
5. Pulse Intro para aceptar la ubicación de inicio predeterminada.
6. Escriba `+512M` para que el tamaño de la partición sea de 1 500 MB (será la partición /boot).
7. Escriba `n` para una nueva partición.
8. Escriba `p` para una partición primaria.
9. Escriba `2` para la partición #2.
10. Pulse Intro para aceptar la ubicación de inicio predeterminada.
11. Escriba `+12288M` para que el tamaño de la partición sea de 2 12 GB (esto supone 8 GB de RAM física). El tamaño recomendado es RAM física + 4 GB (esta será la partición de intercambio).
12. Escriba `n` para una nueva partición.
13. Escriba `p` para una partición primaria.
14. Escriba `3` para la partición #3.
15. Pulse Intro para aceptar la ubicación de inicio predeterminada.
16. Escriba `+10240M` para que el tamaño de la partición sea 3 10 GB (será la partición /boot).
17. Escriba `n` para una nueva partición.
18. Escriba `p` para una partición primaria (se utilizará de forma predeterminada en la partición #4).
19. Pulse Intro para aceptar la ubicación de inicio predeterminada.
20. Pulse Intro para rellenar el tamaño máximo (será la partición /var).
21. Escriba `w` para grabar la tabla de partición en SAN.
22. Escriba `exit` para salir de la modalidad de rescate y reinicie para iniciar la Instalación de la partición personalizada (Paso 3, Instalar la imagen de IBM Security Guardium).

Ejemplos de capturas de pantalla para la configuración de QLogic

Las pantallas de Q-Logic que se muestran aquí representan los pasos necesarios. Se pueden utilizar otras tarjetas de canal de fibra.

1. Modifique el BIOS para la tarjeta QLogic pulsando Ctrl-D. Esta es la primera pantalla que se muestra tras pulsar Ctrl-Q cuando se le solicita entrar en el programa de utilidad de configuración. Esta es una tarjeta de dos puertos. Seleccione el puerto adecuado y pulse Intro.

2. Pulse Intro para cambiar los valores de configuración.



3. Pulse Intro para cambiar los valores del adaptador.

4. Utilice las teclas de flecha para seleccionar BIOS de adaptador de host y pulse Intro para cambiar a Habilitado.

5. Pulse Esc para regresar a la pantalla anterior y utilice la flecha abajo para seleccionar los Valores de arranque seleccionables y pulse Intro.

6. Pulse Intro para cambiar el arranque seleccionable a Habilitado.

7. Seleccione el primer nombre de puerto de arranque, LUN y pulse Intro para ver una lista de los LUN. Si está configurando la tarjeta/puerto correcta, los números de LUN se muestran aquí. Seleccione el primero de la lista.

8. Pulse Esc hasta que haya regresado a la pantalla de reinicio y seleccione reiniciar para rearrancar el sistema. Ahora está preparado para continuar con la instalación de IBM Security Guardium.

Tema principal: Instalación del sistema Guardium

Actualización del sistema Guardium

Utilice esta información para actualizar el sistema IBM Security Guardium a la oferta de V10 más reciente.

Antes de iniciar una actualización, revise las secciones Planificación de una actualización, Elección de un método de actualización y Entornos de versiones mixtas durante una actualización.

Además, están disponibles los recursos siguientes para dar soporte a la experiencia de actualización::

- Hoja de ruta de actualización de alto nivel de IBM Security Guardium: Contiene una visión general de las rutas de actualización soportadas desde varios releases de Guardium.
- IBM Guardium V10.1 Requisitos técnicos de dispositivos de software: Describe los requisitos de hardware para instalaciones de máquinas virtuales y físicas.
- Consejos y sugerencias para la actualización a la versión 10: Proporciona vídeos con información acerca de cómo planificar la actualización, ejecutar la actualización y resolver problemas.

- Planificación de una actualización
  Obtenga información acerca de los diferentes escenarios de actualización e identifique el método correcto para actualizar sus sistemas Guardium con un periodo mínimo de inactividad.
- Tareas de actualización comunes
  Las tareas, tales como depurar los datos del sistema, supervisar las instalaciones y la limpieza después de una actualización, son comunes en todos los escenarios de actualización de Guardium.
- Actualizar un entorno de 32 bits
  Actualice su entorno de Guardium de 32 bits sin utilizar un gestor central de copia de seguridad.
- Actualizar un entorno de 64 bits
  Actualice su entorno de Guardium de 64 bits sin utilizar un gestor central de copia de seguridad.
- Actualizar un entorno de 32 bits sin un gestor central de copia de seguridad
  Actualice su entorno de Guardium de 32 bits utilizando un gestor central de copia de seguridad.
- Actualizar un entorno de 64 bits con un gestor central de copia de seguridad
  Actualice su entorno de Guardium de 64 bits utilizando un gestor central de copia de seguridad.

Planificación de una actualización

Obtenga información acerca de los diferentes escenarios de actualización e identifique el método correcto para actualizar sus sistemas Guardium con un periodo mínimo de inactividad.

- Elección de un método de actualización
  El mejor método para actualizar Guardium depende de varios factores, incluidos la versión desde la que se está actualizando, el hardware del sistema y cualquier requisito de particionamiento especial que tenga.
- Entornos de versiones mixtas durante una actualización
  Durante una actualización, el entorno de Guardium entrará en un estado de versión mixta con funciones restringidas.
- Actualización con gestores centrales y agregadores
  Minimice las interrupciones en el entorno de Guardium siguiendo un método de actualización de arriba a abajo.

Tema principal: Actualización del sistema Guardium

Elección de un método de actualización

El mejor método para actualizar Guardium depende de varios factores, incluidos la versión desde la que se está actualizando, el hardware del sistema y cualquier requisito de particionamiento especial que tenga.

Determine la versión actual de Guardium y el nivel de parche pulsando el icono en la interfaz de usuario principal y seleccionando Acerca de Guardium.

Actualice a la última versión de Guardium utilizando uno de los métodos siguientes:

Parche de actualización
: Utilice un parche de actualización para actualizar todos los sistemas en un entorno gestionado. El parche de actualización conserva todos los datos y las configuraciones con la excepción de las personalizaciones de la IU debido a una nueva arquitectura de IU. Se recomienda la utilización de un parche de actualización sin definir un gestor central de copia de seguridad para entornos de 64 bits con particionamiento predeterminado.

Copia de seguridad, reconstrucción, restauración
: Utilice un método de copia de seguridad, reconstrucción y restauración. Esto requiere realizar una copia de seguridad completa del sistema, reconstruir el sistema a partir de los últimos ISO y restaurar los datos y la configuración del sistema a partir de la copia de seguridad. Se recomienda el uso del método de copia de seguridad, reconstrucción y restauración con un gestor central de copia de seguridad en entornos de 32 bytes o en sistemas con particiones personalizadas.

Importante: Los sistemas particionados personalizados no se pueden actualizar a la V10 utilizando un parche de actualización. En su lugar, debe utilizar el método de copia de seguridad, reconstrucción y restauración. Si existen dudas en relación con el particionamiento de los sistemas, descargue e instale la comprobación de estado p9997. El registro de parches resultante contiene información sobre el particionamiento del sistema.

Utilice las tablas siguientes para identificar el mejor método para actualizar los sistemas a la versión más reciente de Guardium.

Tabla 1. Determinar un método de actualización

Sistema Guardium	**Métodos de actualización para V10**	
	Copia de seguridad de V9, volver a crear el sistema en la V10 más reciente, restaurar desde la copia de seguridad de V9	**Aplicar el parche de actualización más reciente de V10**
V9 parche 600 (64 bits) o posterior	Sí	Sí
V9 parche 600 (32 bits) o posterior	Sí	No
V9.0 parche por debajo de 600	Sí	No
V8.2 o anterior	No	No

Tabla 2. Visión general de las vías de actualización de V10

Nivel de Guardium en el sistema actual	Vía de actualización a la última V10
V8.2	No puede actualizar sistemas V8.2 directamente en sistemas V10. Debe volver a crear los dispositivos con la ISO V9 (64 bits) más reciente y, a continuación, instalar el parche de actualización más reciente de V9 a V10. 1. Crear copia de seguridad del sistema V8.2. 2. Volver a crear el dispositivo con la ISO V9 (64 bits) más reciente. 3. Instalar la GPU V9 parche 600 o posterior (64 bits). 4. Restaurar la copia de seguridad del sistema del sistema V8.2 original. Nota: Para los recopiladores, actualice todos los S-TAP correspondientes a la versión V9 más reciente antes de continuar con el paso siguiente. 5. Instalar la comprobación de estado p9997. 6. Crear una copia de seguridad del sistema V9 (64 bits). 7. Instalar el último parche de actualización de V9 a V10.
V9 (32 bits)	1. Crear una copia de seguridad del sistema V9 (32 bits). 2. Volver a crear el dispositivo con la ISO V10 (64 bits) más reciente. 3. Aplicar la V10 parche 100 o una GPU posterior. 4. Restaurar la copia de seguridad del sistema a partir del sistema V9 (32 bits) original.
V9 por debajo del parche 600 (64 bits)	1. Crear una copia de seguridad del sistema V9 (64 bits). 2. Instalar la GPU V9 parche 600 o posterior (64 bits). 3. Crear una copia de seguridad del sistema V9 (64 bits). 4. Instalar la comprobación de estado p9997. 5. Instalar el último parche de actualización de V9 a V10.
V9 parche 600 (64 bits) o posterior	1. Instalar la comprobación de estado p9997. 2. Crear una copia de seguridad del sistema V9 (64 bits). 3. Instalar el último parche de actualización de V9 a V10.
V10	1. Aplicar la GPU V10 más reciente.

Tema principal: Planificación de una actualización
Conceptos relacionados:
Actualizar un entorno de 32 bits
Actualizar un entorno de 32 bits sin un gestor central de copia de seguridad
Actualizar un entorno de 64 bits
Actualizar un entorno de 64 bits con un gestor central de copia de seguridad

Entornos de versiones mixtas durante una actualización

Durante una actualización, el entorno de Guardium entrará en un estado de versión mixta con funciones restringidas.

Dado que el proceso de actualización no se puede completar en todos los sistemas (gestores, agregadores y recopiladores) y todos los S-TAPs simultáneamente, el entorno de Guardium entrará en un estado de versión mixta durante la actualización. Por ejemplo, después de actualizar un gestor central a la versión V10 más reciente, las unidades gestionadas seguirán funcionando en GPU V9, parche 600. Aunque se da soporte a los entornos de versiones mixtas, se deben tener en cuenta varias limitaciones como parte de cualquier plan de actualización. Por ejemplo, la recopilación de datos, el asesoramiento de datos y las políticas (con algunas restricciones) continuarán funcionando mientras están en un estado mixto, pero las funciones con prestaciones nuevas o mejoradas no funcionarán en un entorno mixto.

Importante: Actualice todo el entorno al último nivel de parche de V10 tan pronto como sea posible. Tenga en cuenta lo siguiente cuando opere en un entorno de versiones mixtas durante la actualización:

- La funcionalidad completa de Guardium no estará disponible hasta que el entorno se haya actualizado a la última versión 10.
- No realice cambios de configuración mientras opera en un entorno de versiones mixtas.
- Guardium V10 no da soporte a entornos mixtos con unidades gestionadas por debajo de GPU V9, parche 600.

Distribución de configuraciones y valores
: La distribución de la configuración no está soportada entre un gestor central V10 y V9 parche 600 o unidades gestionadas posteriores. Esta restricción incluye lo siguiente:

  - Las políticas no se pueden distribuir desde un gestor central V10 a unidades gestionadas V9 parche 600. Las políticas ya instaladas en las unidades gestionadas antes de la actualización permanecen sin cambios.
  - Los valores de parches no se pueden distribuir desde un gestor central V10 a unidades gestionadas de parche 600 V9 o posterior. Los valores de copia de seguridad de parches definidos antes de la actualización permanecen sin cambios.
  - La personalización y distribución del diseño de la IU no se soportan en un gestor central V10 con unidades gestionadas V9 (parche 600 o posterior).

Unidades gestionadas
: No puede registrar unidades gestionadas V9 parche 600 o posterior adicionales después de actualizar el gestor central a V10. Las unidades registradas antes de la actualización permanecen registradas después de la actualización.

Búsqueda rápida
: La búsqueda rápida de empresa funciona en un entorno mixto que consta de un gestor central V10 y unidades gestionadas V9 parche 530 o posterior. La IU debe reiniciarse para poder inicializar de nuevo la búsqueda rápida de empresa. Las unidades gestionadas anteriores a GPU 500 no pueden beneficiarse de la búsqueda de empresa, aunque la búsqueda rápida local sigue estando disponible.
  Si un gestor central se actualiza de V9 a la V10 más recientes y las unidades gestionadas permanecen en la V9, la búsqueda rápida se inhabilita en las unidades gestionadas V9 hasta que las unidades gestionadas se actualizan a V10.

Informes
: Algunos informes generarán errores de SQL o es posible que no muestren los datos correctamente cuando se visualicen en las unidades gestionadas V9 parche 600 o posteriores, incluidas las siguientes:

  - Registro de agregación/archivado

- Conexiones en cuarentena
- Parches instalados
- Motores de inspección inactivos
- Verificación de S-TAP
- Lista de perfilado de conexión
- Estadísticas de reproducción
- Resumen de reproducción

Con la excepción de los datos del *Supervisor de uso de almacenamiento intermedio de empresa*, los datos de las unidades gestionadas V9 parche 600 o posterior no son accesibles en los siguientes informes en un gestor central V10:

- Verificación S-TAP de empresa
- Sucesos de equilibrio de carga de empresa

Tema principal: Planificación de una actualización

Actualización con gestores centrales y agregadores

Minimice las interrupciones en el entorno de Guardium siguiendo un método de actualización de arriba a abajo.

Esto significa actualizar primero un sistema de alto nivel y, a continuación, actualizar los sistemas o agentes que le informan y, a continuación, actualizar el siguiente sistema de alto nivel y los sistemas o agentes que informan al mismo, etc. Este método minimiza el impacto de la operación en un entorno Guardium de versiones mixtas.

Un método de arriba-abajo es necesario debido a que un agregador actualizado puede agregar datos desde releases más antiguos, pero un agregador más antiguo no puede agregar datos desde releases más recientes. De forma similar, un gestor central actualizado puede gestionar unidades que ejecutan releases anteriores, pero las unidades gestionadas no disfrutarán de las funciones completas hasta que se actualicen de modo que coincidan con el gestor central.

Para evitar estos problemas, actualice un gestor central antes de actualizar cualquiera de sus unidades gestionadas. Si tiene varios gestores centrales, primero actualice un gestor central y, a continuación, actualice sus unidades gestionadas antes de actualizar el gestor central siguiente y sus unidades gestionadas.

Del mismo modo, actualice un agregador antes de actualizar cualquier unidad que exporte datos al mismo. Si tiene varios agregadores, primero actualice un agregador y, a continuación, actualice los recopiladores que le informan, antes de pasar a actualizar el siguiente agregador y sus recopiladores.

Finalmente, actualice un recopilador antes de actualizar los S-TAPs registrado. Actualice un recopilador y todos los S-TAPs registrados antes de actualizar el siguiente recopilador y su S-TAPs.

Este método proporciona sistemas compatibles, desde gestores centrales a agregadores, recopiladores y S-TAPs, en cada una de las ramas de su entorno más rapidez que cuando se actualizan todos los agregadores o gestores centrales antes de actualizar los recopiladores.

Tema principal: Planificación de una actualización

Tareas de actualización comunes

Las tareas, tales como depurar los datos del sistema, supervisar las instalaciones y la limpieza después de una actualización, son comunes en todos los escenarios de actualización de Guardium.

- Depurar datos del sistema
  La depuración de datos innecesarios del sistema Guardium puede acelerar significativamente el proceso de actualización.
- Instalación, distribución y supervisión de parches
  Antes de comenzar una actualización, es útil familiarizarse con el modo de cargar e instalar los parches, supervisar las instalaciones de los parches y verificare que las instalaciones se han realizado correctamente.
- Seguimiento del progreso de la instalación con diag
  Utilice el mandato `diag` para acceder al registro de actualización y realizar un seguimiento del progreso de una actualización.
- Verificación y limpieza después de la actualización
  Verifique que la actualización se ha completado correctamente y realice el mantenimiento posterior a la actualización.

Tema principal: Actualización del sistema Guardium

Depurar datos del sistema

La depuración de datos innecesarios del sistema Guardium puede acelerar significativamente el proceso de actualización.

Acerca de esta tarea

Para obtener el mejor rendimiento y minimizar los riesgos asociados con la actualización de grandes cantidades de datos, intente conseguir menos del 20% de uso interno de la base de datos depurando los datos innecesarios del sistema.

Procedimiento

1. Abra Gestionar > Gestión de datos > Archivado de datos.
2. Pulse el recuadro de selección Depurar para definir una operación de depuración.
   Importante: Los cambios realizados en la configuración de depuración de Archivado de datos también se aplican a la configuración de la depuración de exportación de datos.
3. Defina un periodo de tiempo para Depurar datos anteriores a. Todos los datos con una antigüedad superior al periodo de días, semanas o meses especificados se depurarán del sistema.
4. Pulse el recuadro de selección Permitir depurar sin exportar ni archivar.
5. Pulse Guardar para guardar los cambios de la configuración.
6. Pulse Ejecutar una vez ahora para ejecutar la depuración y depurar los datos del sistema antiguo.

Qué hacer a continuación

Abra Gestionar > Informes > Supervisión de actividad > Trabajos planificados para supervisar el estado del trabajo de archivado de datos.
Tema principal: Tareas de actualización comunes

Instalación, distribución y supervisión de parches

Antes de comenzar una actualización, es útil familiarizarse con el modo de cargar e instalar los parches, supervisar las instalaciones de los parches y verificare que las instalaciones se han realizado correctamente.

Instalar un parche utilizando scp

Cuando actualiza el entorno de Guardium, hay varias formas de cargar e instalar parches en gestores centrales y unidades gestionadas.

Importante: Los parches bajados en formato ZIP se deben desempaquetar fuera del sistema Guardium antes de subirlos y de la instalación. Tenga en cuenta las siguientes restricciones para los parches con cambios en la estructura de la base de datos:

- Realice o planifique la instalación del parche cuando haya poca actividad en el sistema Guardium para evitar conflictos con procesos de larga ejecución como, por ejemplo, informes con mucha información, procesos de auditoría, copias de seguridad e importaciones.
- El tiempo exacto necesario para la instalación del parche depende de la utilización de la base de datos, la distribución de los datos y de otras consideraciones.
- Instale los parches de forma jerárquica, de arriba a abajo, aplicando primero los parches al gestor central, luego a los agregadores y por último a los recopiladores.

Para cargar e instalar un parche utilizando `scp`, emita el siguiente mandato de CLI: `store system patch install scp`

Cuando se complete la carga, se le solicitará automáticamente que continúe con la instalación del parche.

Instalar un parche utilizando fileserver

Para cargar e instalar un parche utilizando el mandato fileserver de Guardium:

1. Inicialice el servidor de archivos utilizando el siguiente mandato de CLI: `fileserver [ip_address]`, donde `[ip_address]` es el sistema que se utiliza para conectarse al sistema Guardium.
2. En un navegador web, conéctese al sistema Guardium.
   a. Pulse Subir parche.
   b. Examine para seleccionar el archivo de parche y, a continuación, pulse Subir.
3. Emita el siguiente mandato de CLI para instalar el parche: `store system patch install system`.

Distribuir un parche

Para distribuir un parche desde un gestor central a unidades gestionadas, se debe haber realizado una de las acciones siguientes:

- Instalar el parche en el gestor central
- Ejecutar el mandato de CLI `store system patch available` para que el parche esté disponible en el gestor central.

Distribuir el parche a las unidades gestionadas utilizando la página Gestión central en el gestor central. Vaya a Gestionar > Gestión central > Gestión central y pulse Distribución de parches.

Supervisar y verificar la instalación de parches

Puede supervisar y verificar la instalación de los parches de las siguientes maneras:

- Emita el mandato de CLI siguiente: `show system patch install`.
- Utilice la página Gestión central en el CM: Gestionar > Gestión central > Gestión central > Estado de instalación de parches.

Importante: Los parches de la versión 9 no estarán disponibles después de que se haya actualizado el sistema Guardium a la versión 10.
Tema principal: Tareas de actualización comunes

Seguimiento del progreso de la instalación con diag

Utilice el mandato `diag` para acceder al registro de actualización y realizar un seguimiento del progreso de una actualización.

Procedimiento

1. Inicie sesión en la CLI del sistema de Guardium.
2. Emita el mandato `diag`.
3. En el menú de mandatos de `diag`:
   a. Seleccione 1 Gestión de salida y pulse Aceptar.
   b. Seleccione 3 Exportar archivos de registro y pulse Aceptar.
   c. Seleccione los archivos de registro que necesite y pulse Aceptar.
   d. Seleccione 1 FTP o 2 SCP y pulse Aceptar.
   e. Especifique el nombre de host en el que desee realizar la carga y pulse Aceptar.
   f. Especifique el nombre de usuario y pulse Aceptar.
   g. Especifique la contraseña y pulse Aceptar.
   Nota: Si se selecciona 2 SCP, se solicita la vía de acceso de destino antes que la contraseña.
   h. Especifique la vía de acceso de destino y pulse Aceptar.
   i. Compruebe la información y pulse Aceptar. Se carga el archivo en el sistema de destino.
   j. Seleccione Aceptar para salir.
   k. Seleccione 3 Salir y pulse Aceptar.
   Nota: Vuelva a **3a** si necesita cargar otro archivo, de lo contrario continúe en el paso siguiente.
   l. Seleccione 5 Salir a CLI y pulse Aceptar.

Tema principal: Tareas de actualización comunes

Verificación y limpieza después de la actualización

Verifique que la actualización se ha completado correctamente y realice el mantenimiento posterior a la actualización.

Procedimiento

1. Si ha realizado la actualización utilizando un parche de actualización, inicie sesión como usuario de CLI y emita el mandato siguiente: `show upgrade-status`. El mandato generará información de estado detallada del proceso de actualización, y la última línea de la salida deberá indicar `INFO:Migration Complete`.
2. Si ha actualizado un gestor central, verifique que las unidades gestionadas estén listadas en la página Gestionar > Gestión central > Gestión central.
3. Verifique que los informes personalizados creados en versiones anteriores de Guardium estén disponibles en Informes > Mis informes personalizados.

   Mis informes personalizados debe contener todos los informes nuevos que haya creado, así como los informes predefinidos que haya modificado en una versión anterior de Guardium.

4. Renueve todas las unidades gestionadas en la página Gestión central para poder distribuir las licencias a las MU actualizadas.
5. Es posible que tenga que actualizar el archivo DPS de Guardium después de los procedimientos de actualización o restauración. Descargue el archivo DPS más reciente y, a continuación, utilice la herramienta Reforzar > Asesoramiento de vulnerabilidades > Subidas de cliente para subir e importar el nuevo archivo DPS.
6. Es posible que sea necesario volver a cargar los logotipos de empresa antes de los procedimientos de actualización o restauración. Para volver a cargar un logotipo de cliente, siga estos pasos:
   a. Inicie sesión como usuario admin.
   b. Vaya a Configurar > Herramientas y vistas > Perfil global.
   c. Busque el archivo del logotipo de empresa.
   d. Suba el archivo de logotipo.
7. Verifique el estado de los servicios CSRF (Cross-Site Request Forgery) y XSS (Cross-Site Scripting) utilizando los mandatos de CLI show gui csrf_status y show gui xss_status.

Tema principal: Tareas de actualización comunes

Actualizar un entorno de 32 bits

Actualice su entorno de Guardium de 32 bits sin utilizar un gestor central de copia de seguridad.

Antes de actualizar el entorno de Guardium de 32 bits mediante ISO, sin utilizar un gestor central de copia de seguridad, revise la siguiente lista de comprobación y complete cada elemento antes de intentar la actualización.

Importante: Antes de ejecutar `restore db` en un sistema de la V10, aplique los últimos parches de mantenimiento después de que se haya compilado su sistema para la V10.Si está utilizando un gestor central basado en recopiladores de 32 bits, debe volver a compilarlo para una gestor central basado en recopiladores de 64 bits antes de actualizarlo a la V10.

Lista de comprobación de actualización

- Descargue el último parche de comprobación de salud (p9997) desde Fix Central. Para obtener más información, consulte Notas del release del parche de comprobación de salud de Guardium.
- Los sistemas actuales deben estar en el nivel de Guardium V9 y tener una arquitectura de 32 bits.
- Descargue el último release de Guardium V9 o descárguelo más tarde desde Fix Central [opcional].
- Descargue el último Guardium V10 ISO desde Passport Advantage
- Descargue todas las licencias base y licencias de adición desde Passport Advantage
- Descargue la última GPU para la V10 desde Fix Central, si hay una disponible
- Registre todos los parámetros de configuración de red devueltos por los siguientes mandatos de CLI de Guardium:

```
show network interface all
show network route defaultroute
show network resolver 1
show system hostname
show system domain
```

1. Actualizar un gestor central de 32 bits
   Cuando actualice el entorno de Guardium de 32 bits, siga estos pasos para ejecutar el parche de comprobación de estado y actualizar un gestor central mediante un procedimiento de copia de seguridad, reconstrucción y restauración.
2. Actualizar unidades gestionadas de 32 bits
   Actualice las unidades gestionadas de 32 bits utilizando un procedimiento de copia de seguridad, recompilación y restauración.

Tema principal: Actualización del sistema Guardium
Conceptos relacionados:
Planificación de una actualización

Actualizar un gestor central de 32 bits

Cuando actualice el entorno de Guardium de 32 bits, siga estos pasos para ejecutar el parche de comprobación de estado y actualizar un gestor central mediante un procedimiento de copia de seguridad, reconstrucción y restauración.

Antes de empezar

Complete la lista de comprobación de la actualización de la sección Actualizar un entorno de 32 bits.

Procedimiento

1. Actualice el sistema a la versión 9, parche 600 o posterior.
2. Establezca la hora en el huso horario local y sincronice la hora en todos los sistemas Guardium utilizando un servidor NTP.

3. Descargue e instale el parche de comprobación de estado más reciente (p9997) y verifique que la instalación se ha realizado correctamente. Consulte el apartado Instalación, distribución y supervisión de parches para obtener instrucciones.
4. Realice una copia de seguridad del sistema del gestor central y verifique que se ha realizado correctamente.
   a. Vaya a Gestionar > Gestión de datos > Copia de seguridad del sistema.
   b. Configure el protocolo en función de sus preferencias y rellene todos los campos.
   c. Realice una copia de seguridad de la configuración y los datos.

   Importante: Cree al menos una copia de seguridad válida antes de empezar el procedimiento de actualización.
5. Monte el ISO más reciente de Guardium V10.
   a. Seleccione un tipo de sistema en los primeros cinco segundos de entrar en el instalador de Guardium. La selección predeterminada es Instalación estándar (no CM) con un tipo de unidad de recopilador autónomo. Cuando actualice un gestor central o un agregador, seleccione Agregador .
   b. Permita que se complete la instalación y se reinicie el sistema.
6. Configure los parámetros de red. Inicie sesión en la CLI de Guardium y emita los mandatos siguientes:

```
store network interface ip
store network route defaultroute
store network resolver 1
store system hostname
store system domain
```

7. Inicie sesión en la interfaz de usuario de Guardium y valide los componentes predeterminados.
   Nota: Si inicia sesión por primera vez, la contraseña predeterminada es `guardium`.
   a. Verifique que solo estén visibles los elementos de navegación Bienvenido y Configuración.
   b. Vaya a Configurar > Herramientas y vistas > Licencia o pulse el icono para verificar que no hay ninguna licencia instalada en el sistema.
8. Instale las licencias.
   a. Vaya a la página de licencia siguiendo el enlace de notificación o seleccionando Configuración > Herramientas y vistas > Licencia.
   b. Aplique todas las licencias base relevantes y licencias añadidas y acepte los acuerdos de licencia.
   c. Si es necesario, cambie el tipo de unidad del sistema iniciando sesión en CLI y emitiendo el siguiente mandato de CLI: `store unit type <type>` donde `<type>` es `manager`, `standalone`, `netinsp`, `mainframe`, `sink` o `stap`.
9. Instale la GPU V10 más reciente (si es más reciente que el ISO V10 más reciente) y los últimos parches de mantenimiento del gestor central y verifique que se han instalado correctamente.
10. Restaure los datos y las configuraciones en el gestor central.
    a. Emita el mandato siguiente de CLI de Guardium para importar los archivos: `import file`.
    b. Importe los datos y los archivos de configuración por separado.
    c. Realice la restauración de datos y de la configuración con el siguiente mandato de CLI: `restore db-from-prev-version`.

    Consejo: Se puede acceder al registro de restore db ejecutando el mandato de CLI `diag`. Consulte la sección Seguimiento del progreso de la instalación con diag para obtener más información.
11. Después de restaurar los datos y las configuraciones en el gestor central, verifique que toda la información de las unidades gestionadas relevantes se visualiza en la página Gestión central.
12. Valide que el entorno gestionado funciona según lo previsto.
    a. Verifique que se hayan restaurado los informes personalizados
    b. Verifique que las unidades gestionadas estén en línea y son accesibles desde la página Gestión central

    Atención: Tenga en cuenta las limitaciones previstas cuando ejecuta en un entorno mixto. Para obtener más información, consulte Entornos de versiones mixtas durante una actualización.

Qué hacer a continuación

Después de actualizar correctamente el gestor central de Guardium de 32 bits, consulte Actualizar unidades gestionadas de 32 bits.
Tema principal: Actualizar un entorno de 32 bits
Tema siguiente: Actualizar unidades gestionadas de 32 bits

Actualizar unidades gestionadas de 32 bits

Actualice las unidades gestionadas de 32 bits utilizando un procedimiento de copia de seguridad, recompilación y restauración.

Antes de empezar

Antes de actualizar las unidades gestionadas de 32 bits, revise y complete las tareas siguientes:

- Actualizar un entorno de 32 bits
- Actualizar un gestor central de 32 bits

Importante: Debe actualizar el entorno al parche 600 V9 o posterior antes de actualizar a la V10 más reciente.

Procedimiento

1. Distribuya el parche más reciente de Comprobación de salud (p9997) para las unidades gestionadas y verifique que la instalación se ha realizado correctamente. Consulte la sección Instalación, distribución y supervisión de parches para obtener más información.
2. Realice copias de seguridad de todas las unidades gestionadas.
3. Vuelva a crear las unidades gestionadas utilizando el procedimiento siguiente:
   a. Monte la imagen de ISO más reciente de Guardium V10.
   b. Seleccione un tipo de sistema a los cinco segundos de entrar en el instalador de Guardium. Utilice la selección predeterminada Instalación estándar (no CM) con un tipo de unidad de recopilador autónomo.
   c. Permita que se complete la instalación y se reinicie el sistema.
4. Configure los parámetros de red. Inicie sesión en la CLI de Guardium y emita los mandatos siguientes:

```
store network interface ip
store network route defaultroute
store network resolver 1
store system hostname
store system domain
```

5. Inicie sesión en la interfaz de usuario de Guardium y verifique no haya licencias instaladas en el sistema.
   Consejo:
   - Si inicia sesión por primera vez, la contraseña predeterminada es `guardium`.
   - Si está trabajando con un sistema autónomo que finalmente se convertirá en una unidad gestionada, no es necesario instalar licencias.

   a. En la navegación principal de Guardium, verifique que solo estén visibles los elementos de navegación Bienvenido y Configuración.
   b. Vaya a Configurar > Herramientas y vistas > Licencia o pulse el icono para verificar que no hay ninguna licencia instalada en el sistema.
6. Restaure los datos y las configuraciones en las unidades gestionadas.
   Nota: Cuando se restaura una unidad gestionada desde una copia de seguridad, los diseños personalizados para dicha unidad gestionada se perderán si el gestor central está inactivo en el momento de la restauración.
   a. Emita el mandato siguiente de CLI de Guardium para importar los archivos: `import file`.
   b. Importe los datos y los archivos de configuración por separado.
   c. Realice la restauración de datos y de la configuración con el siguiente mandato de CLI: `restore db-from-prev-version`.
7. Cuando todas las unidades gestionadas se hayan actualizado correctamente, distribuya las licencias desde el gestor central a las unidades gestionadas.
   a. Inicie sesión en la interfaz de usuario del gestor central.
   b. Vaya a Gestión central > Gestionar > Gestión central y verifique que se listan las unidades gestionadas.
   c. Pulse el recuadro de selección Seleccionar todo para seleccionar todas las unidades gestionadas.
   d. Pulse el botón Renovar para distribuir las licencias a las unidades gestionadas.
   e. Espere hasta que se complete el proceso de renovación.
   f. Inicie sesión en la interfaz de usuario de las unidades gestionadas y vaya a Configuración > Herramientas y vistas > Licencia para verificar que se han instalado las licencias correctas. Cuando se hayan instalado las licencias correctas:
      - Las opciones de menú de navegación esperadas estarán disponibles en las unidades gestionadas.
      - Los informes sobre las unidades gestionadas serán funcionales.
      - Se podrá acceder a los informes a través de orígenes de datos remotos desde el gestor central.
8. Si se han instalado la GPU V10 más reciente (si es más nueva que ISO V10 más reciente) y los parches de mantenimiento en el gestor central, distribuye la GPU y los parches en las unidades gestionadas.
9. Si utiliza herramientas de VMware, debe volver a instalar estas herramientas después de completar la actualización. Para volver a instalar las Herramientas de VMware, inicie sesión en la CLI de Guardium, emita el siguiente mandato y siga las solicitudes: `setup vmware_tools install`.

Resultados

Ha completado correctamente una actualización de su entorno Guardium de 32 bits a la versión más reciente de V10. Verifique la estabilidad del entorno Guardium.
Tema principal: Actualizar un entorno de 32 bits
Tema anterior: Actualizar un gestor central de 32 bits

Actualizar un entorno de 64 bits

Actualice su entorno de Guardium de 64 bits sin utilizar un gestor central de copia de seguridad.

Antes de actualizar el entorno de Guardium de 64 bits mediante ISO, sin utilizar un gestor central de copia de seguridad, revise la siguiente lista de comprobación y complete cada elemento antes de intentar la actualización.

Importante: Antes de ejecutar `restore db` en un sistema de la V10, aplique los últimos parches de mantenimiento después de que se haya compilado su sistema para la V10. Si está utilizando un gestor central basado en recopiladores de 64 bits, el parche de actualización se encargará de actualizar y convertirá el sistema desde un gestor central basado en recopiladores en un gestor central basado en agregadores.

Lista de comprobación de actualización

- Los sistemas actuales deben estar en el nivel de Guardium V9, parche 600, y tener una arquitectura de 64 bits.
- Descargue el último release de Guardium V9 o descárguelo más tarde desde Fix Central [opcional].
- Descargar el parche de actualización p10000
- Descargue los parches de mantenimiento más recientes desde Fix Central
- Descargue el último parche de comprobación de salud (p9997) desde Fix Central. Para obtener más información, consulte Notas del release del parche de comprobación de salud de Guardium.

Para planificar la contingencia, descargue lo siguiente:

- Todas las licencias base y de adición necesarias.
- El ISO de V10 más reciente desde Passport Advantage.

1. Actualizar un gestor central de 64 bits
   Cuando actualice el entorno de Guardium de 64 bits, siga estos pasos para ejecutar el parche de comprobación de estado y actualizar un gestor central.
2. Actualizar unidades gestionadas de 64 bits
   Actualice las unidades gestionadas de 64 bits utilizando un parche de actualización.

Tema principal: Actualización del sistema Guardium
Conceptos relacionados:
Planificación de una actualización

Actualizar un gestor central de 64 bits

Cuando actualice el entorno de Guardium de 64 bits, siga estos pasos para ejecutar el parche de comprobación de estado y actualizar un gestor central.

Antes de empezar

Complete la lista de comprobación de la actualización de la sección Actualizar un entorno de 64 bits.

Procedimiento

1. Actualice el sistema a la versión 9, parche 600 o posterior.

2. Establezca la hora en el huso horario local y sincronice la hora en todos los sistemas Guardium utilizando un servidor NTP.
3. Descargue e instale el parche de comprobación de estado más reciente (p9997) y verifique que la instalación se ha realizado correctamente. Consulte el apartado Instalación, distribución y supervisión de parches para obtener instrucciones.
4. Realice una copia de seguridad del sistema del gestor central y verifique que se ha realizado correctamente.
   a. Vaya a Gestionar > Gestión de datos > Copia de seguridad del sistema.
   b. Configure el protocolo en función de sus preferencias y rellene todos los campos.
   c. Realice una copia de seguridad de la configuración y los datos.

   Importante: Cree al menos una copia de seguridad válida antes de empezar el procedimiento de actualización.
5. Instale p10000 en el gestor central y supervise su instalación.
   Importante: Una vez realizada la instalación del parche, el proceso de actualización se inicia automáticamente y se reinicia el sistema. No reinicie manualmente el sistema.
6. Permita que finalice la instalación del sistema operativo.
   - El tiempo de instalación depende de la cantidad de datos implicados, así como de la configuración y las especificaciones del sistema
   - Una vez completada la instalación del sistema operativo, el sistema rearranca por primera vez en Guardium V10 más reciente.
     Atención: Después de instalar correctamente la Versión 10 más reciente, el primer arranque del sistema va seguido de:
     - Configuración de red, migración de datos de base de datos, inicio de base de datos.
     - Actualización de licencia, actualización de PSML y ajuste del idioma.
     - Reinicio de base de datos, migración de certificados y claves, migración de contraseña y limpieza de archivos.
7. Confirme que el gestor central se ha actualizado satisfactoriamente:
   a. Inicie sesión en la CLI de Guardium. Si la CLI entra en modalidad de recuperación, la actualización aún está en curso.
   b. Emita el mandato de CLI siguiente: show upgrade-status El mandato también se puede emitir desde la modalidad de recuperación de CLI.
   c. Verifique que la última línea de la salida sea: 5.0:INFO:Migration Complete
   d. Si todavía está en modalidad de recuperación de CLI, salga de la CLI y vuelva a iniciar sesión para entrar en la modalidad normal de CLI de Guardium.
   e. Emita el mandato de CLI siguiente: show system patch install
   f. Verifique que el estado de p10000 es el siguiente: Fase 5: Migración completada
8. Inicie sesión en la interfaz de usuario de Guardium y acepte los acuerdos de licencia para habilitar las características del producto.
   a. Vaya a Configurar > Herramientas y vistas > Licencia.
   b. Acepte el acuerdo de licencia base.
   c. Acepte todos los acuerdos de licencia adicionales.

   Nota: Omitir este paso evita que las funciones de Guardium estén habilitadas.
9. Valide que el entorno gestionado funciona según lo previsto, verificando que las unidades gestionadas aparecen en línea y son accesibles desde la página Gestión central.
   Atención: Tenga en cuenta las limitaciones previstas cuando ejecuta en un entorno mixto. Para obtener más información, consulte Entornos de versiones mixtas durante una actualización.
10. Instale los parches de mantenimiento más recientes en el gestor central y verifique que se han instalado correctamente.

Qué hacer a continuación

Después de actualizar correctamente el gestor central de Guardium de 64 bits, consulte Actualizar unidades gestionadas de 64 bits.
Tema principal: Actualizar un entorno de 64 bits
Tema siguiente: Actualizar unidades gestionadas de 64 bits

Actualizar unidades gestionadas de 64 bits

Actualice las unidades gestionadas de 64 bits utilizando un parche de actualización.

Antes de empezar

Antes de actualizar las unidades gestionadas de 64 bits utilizando un parche de mantenimiento, revise y complete las tareas siguientes:

- Actualizar un entorno de 64 bits
- Actualizar un gestor central de 64 bits

Importante: Debe actualizar el entorno al parche 600 V9 o posterior antes de actualizar a la V10 más reciente.

Procedimiento

1. Distribuya el parche más reciente de Comprobación de salud (p9997) para las unidades gestionadas y verifique que la instalación se ha realizado correctamente. Consulte la sección Instalación, distribución y supervisión de parches para obtener más información.
2. Realice copias de seguridad de todas las unidades gestionadas.
3. Distribuya el parche de actualización de p10000 a todas las unidades gestionadas y supervise la instalación del parche. Lea la sección Instalación, distribución y supervisión de parches para obtener más información.
   Atención: Una vez realizada la instalación del parche, el proceso de actualización se inicia automáticamente y se reinicia el sistema. No reinicie manualmente el sistema.
   El tiempo necesario para la actualización depende de la cantidad de datos implicados, así como de la configuración y las especificaciones del sistema. Cuando se completa la actualización y el sistema se reinicia, el primer arranque del sistema actualizado va seguido de:
   - Configuración de red, migración de datos de base de datos, inicio de base de datos.
   - Actualización de licencia, actualización de PSML y ajuste del idioma.
   - Reinicio de base de datos, migración de certificados y claves, migración de contraseña y limpieza de archivos.

   Durante este proceso, no podrá iniciar la sesión en unidades gestionadas actualizadas hasta que finalice la migración de la base de datos.
4. Verifique que el proceso de actualización se haya completado correctamente en cada unidad gestionada.
   a. Inicie sesión en la CLI de Guardium del sistema que se está actualizando. Si la CLI entra en modalidad de recuperación, la actualización aún está en curso.
   b. Emita el mandato de CLI siguiente: `show upgrade-status`. Este mandato también se puede emitir desde la modalidad de recuperación de CLI.
   c. Verifique que la última línea de la salida sea: `5.0:INFO:Migration Complete`.
   d. Si está en modalidad de recuperación de CLI, salga de la CLI y vuelva a iniciar sesión para entrar en la modalidad de CLI.
   e. Emita el mandato de CLI siguiente: `show system patch install`.
      Atención: El mandato `show system patch install` no devuelve resultados hasta que se completa la actualización, después del primer reinicio.
   f. Verifique que el estado de instalación del parche de actualización sea: `Fase 5: Migración completada`.
5. Cuando todas las unidades gestionadas se hayan actualizado correctamente, distribuya las licencias desde el gestor central a las unidades gestionadas.

a. Inicie sesión en la interfaz de usuario del gestor central.
b. Vaya a Gestión central > Gestionar > Gestión central y verifique que se listan las unidades gestionadas.
c. Pulse el recuadro de selección Seleccionar todo para seleccionar todas las unidades gestionadas.
d. Pulse el botón Renovar para distribuir las licencias a las unidades gestionadas.
e. Espere hasta que se complete el proceso de renovación.
f. Inicie sesión en la interfaz de usuario de las unidades gestionadas y vaya a Configuración > Herramientas y vistas > Licencia para verificar que se han instalado las licencias correctas. Cuando se hayan instalado las licencias correctas:
   - Las opciones de menú de navegación esperadas estarán disponibles en las unidades gestionadas.
   - Los informes sobre las unidades gestionadas serán funcionales.
   - Se podrá acceder a los informes a través de orígenes de datos remotos desde el gestor central.

6. Si se han instalado la última GPU para V10 y cualquier parche de mantenimiento en el gestor central, distribuya los parches de GPU y de mantenimiento a las unidades gestionadas.
7. Si utiliza herramientas de VMware, debe volver a instalar estas herramientas después de completar la actualización. Para volver a instalar las Herramientas de VMware, inicie sesión en la CLI de Guardium, emita el siguiente mandato y siga las solicitudes: `setup vmware_tools install`.

Resultados

Ha completado correctamente una actualización de su entorno Guardium de 64 bits a la versión más reciente de V10. Verifique la estabilidad del entorno Guardium.
Tema principal: Actualizar un entorno de 64 bits
Tema anterior: Actualizar un gestor central de 64 bits

Actualizar un entorno de 32 bits sin un gestor central de copia de seguridad

Actualice su entorno de Guardium de 32 bits utilizando un gestor central de copia de seguridad.

Antes de actualizar el entorno de Guardium de 32 bits, utilizando un gestor central de copia de seguridad, revise la siguiente lista de comprobación y complete cada elemento antes de intentar la actualización.

Importante: Antes de ejecutar `restore db` en un sistema de la V10, aplique los últimos parches de mantenimiento después de que se haya compilado su sistema para la V10.Si está utilizando un gestor central basado en recopiladores de 32 bits, debe volver a compilarlo para una gestor central basado en recopiladores de 64 bits antes de actualizarlo a la V10.

Lista de comprobación de actualización

- Identifique y registre todas las unidades gestionadas definidas en el entorno actual.
- Descargue el último parche de comprobación de salud (p9997) desde Fix Central. Para obtener más información, consulte Notas del release del parche de comprobación de salud de Guardium.
- Los sistemas actuales deben estar en el nivel de Guardium V9 y tener una arquitectura de 32 bits.
- Descargue el último release de Guardium V9 o descárguelo más tarde desde Fix Central [opcional].
- Descargue el último Guardium V10 ISO desde Passport Advantage
- Descargue todas las licencias base y licencias de adición desde Passport Advantage
- Descargue la última GPU para la V10 desde Fix Central, si hay una disponible
- Registre todos los parámetros de configuración de red devueltos por los siguientes mandatos de CLI de Guardium:

```
show network interface all
show network route defaultroute
show network resolver 1
show system hostname
show system domain
```

1. Actualizar un gestor central de copia de seguridad de 32 bits
   Cuando actualice el entorno de Guardium de 32 bits, siga estos pasos para ejecutar el parche de comprobación de estado y actualizar un gestor central de copia de seguridad mediante un procedimiento de copia de seguridad, reconstrucción y restauración.
2. Actualizar el gestor central primario de 32 bits antiguo
   Cuando trabaje con un gestor central de copia de seguridad, siga estos procedimientos para actualizar el gestor central primario de 32 bits antiguo mediante un procedimiento de copia de seguridad, recompilación y restauración.
3. Actualizar unidades gestionadas de 32 bits
   Actualice las unidades gestionadas de 32 bits utilizando un procedimiento de copia de seguridad, recompilación y restauración.

Tema principal: Actualización del sistema Guardium
Conceptos relacionados:
Planificación de una actualización

Actualizar un gestor central de copia de seguridad de 32 bits

Cuando actualice el entorno de Guardium de 32 bits, siga estos pasos para ejecutar el parche de comprobación de estado y actualizar un gestor central de copia de seguridad mediante un procedimiento de copia de seguridad, reconstrucción y restauración.

Antes de empezar

Complete la lista de comprobación de la actualización de la sección Actualizar un entorno de 32 bits sin un gestor central de copia de seguridad.

Procedimiento

1. Actualice el sistema a la versión 9, parche 600 o posterior.
2. Establezca la hora en el huso horario local y sincronice la hora en todos los sistemas Guardium utilizando un servidor NTP.
3. Descargue e instale el parche de comprobación de estado más reciente (p9997) y verifique que la instalación se ha realizado correctamente. Consulte el apartado Instalación, distribución y supervisión de parches para obtener instrucciones.
   Importante: Necesitará instalar el parche de comprobación de estado más reciente (p9997) en el gestor central primario y en el gestor central de copia de seguridad candidato antes de designar un gestor central de copia de seguridad.

4. Defina un nuevo gestor central de copia de seguridad.
    a. Vaya a la página Gestión central en el gestor central primario.
    b. Seleccione un agregador gestionado.
    c. Verifique que el gestor central primario y el gestor central de copia de seguridad candidato tengan instalados los mismos parches.
    d. Designe el agregador como un gestor central de copia de seguridad.
    e. Verifique que el archivo cm_sync_file.tgz se haya creado, comprobando el Registro de agregación/archivado en el nuevo gestor central.
5. Realice una copia de seguridad del sistema del gestor central de copia de seguridad y verifique que se ha realizado correctamente.
    a. Vaya a Gestionar > Gestión de datos > Copia de seguridad del sistema.
    b. Configure el protocolo en función de sus preferencias y rellene todos los campos.
    c. Asegúrese de que realiza una copia de seguridad de la configuración y los datos.

   Importante: Cree al menos una copia de seguridad válida antes de empezar el procedimiento de actualización.
6. Vuelva a crear el gestor central de copia de seguridad utilizando el ISO V10 más reciente.
    a. Monte el ISO V10 más reciente.
    b. Seleccione un tipo de sistema en los primeros cinco segundos de entrar en el instalador de Guardium. La selección predeterminada es Instalación estándar (no CM) con un tipo de unidad de recopilador autónomo.
7. Permita que se complete la instalación y se reinicie el sistema.
8. Configure los parámetros de red. Inicie sesión en la CLI de Guardium y emita los mandatos siguientes:

```
store network interface ip
store network route defaultroute
store network resolver 1
store system hostname
store system domain
```

9. Inicie sesión en la interfaz de usuario de Guardium y valide los componentes predeterminados.
   Nota: Si inicia sesión por primera vez, la contraseña predeterminada es `guardium`.
    a. Verifique que solo estén visibles los elementos de navegación Bienvenido y Configuración.
    b. Vaya a Configurar > Herramientas y vistas > Licencia o pulse el icono para verificar que no hay ninguna licencia instalada en el sistema.
10. Instale la licencia.
    a. Vaya a la página de licencia siguiendo el enlace de la notificación o seleccionando Configuración > Herramientas y vistas > Licencia.
    b. Aplique todas las licencias base relevantes y licencias añadidas y acepte los acuerdos de licencia.
11. Instale la GPU V10 más reciente (si es más reciente que el ISO V10 más reciente) y los últimos parches de mantenimiento del gestor central y verifique que se han instalado correctamente.
12. Establezca el secreto compartido en el gestor central de copia de seguridad utilizando el mandato de CLI `store system shared secret` mediante Configurar > Herramientas y vistas > Sistema.
13. Restaure los datos y las configuraciones en el gestor central.
    a. Emita el mandato siguiente de CLI de Guardium para importar los archivos: `import file`.
    b. Importe los datos y los archivos de configuración por separado.
    c. Realice la restauración de datos y de la configuración con el siguiente mandato de CLI: `restore db-from-prev-version`.

    Consejo: Se puede acceder al registro de restore db ejecutando el mandato de CLI `diag`. Consulte la sección Seguimiento del progreso de la instalación con diag para obtener más información.
14. Desde el gestor central primario, verifique que el gestor central de copia de seguridad V10 está disponible y en línea. Identifique y anote el número de unidades gestionadas que informan al gestor central primario (esta información se utiliza después de realizar la transición al gestor central de copia de seguridad).
    Importante: El gestor central de copia de seguridad (que ahora ejecuta el último Guardium V10) puede mostrar una luz de estado de color rojo. Esto sucede cuando el gestor central envía una señal V9 a un sistema V10 y falla, y puede seguir promocionando el servidor siempre que el archivo de sincronización del gestor central esté presente en el gestor central de copia de seguridad. No intente realizar una renovación.
15. Verifique que el archivo cm_sync_file.tgz haya completado al menos dos transferencias correctas desde el gestor central primario al gestor central de copia de seguridad, comprobando el Registro de agregación/archivado en el gestor central primario. Las transferencias deben realizarse a intervalos de 30 minutos.
16. Convierta el gestor central de copia de seguridad en el gestor central primario. Es posible que se muestre el siguiente mensaje después de iniciar sesión en el gestor central de copia de seguridad:

```
La versión del gestor central es inferior a la versión de esta unidad gestionada. La funcionalidad está limitada hasta que se corrija la discordancia de versiones.
```

    a. Vaya a Configurar > Gestión de datos.
    b. Pulse Convertir en CM primario. Si no ve esta opción, verifique que cm_sync_file se haya transferido correctamente.
    c. Responda Sí al mensaje: ¿Está seguro de que desea hacer que esta unidad sea el gestor central (CM) primario?
    d. Pulse Cerrar en el mensaje emergente: El cambio tardará unos minutos y requerirá reiniciar la interfaz gráfica de usuario. Se cerrará la sesión cuando se realice el reinicio de la GUI. El icono de progreso se muestra en la página de la interfaz de usuario.

    Nota: Durante el proceso de conversión, la interfaz de usuario de Guardium no está disponible temporalmente. Una vez completado el proceso, la pantalla de inicio de sesión vuelve al estado normal.
17. Efectúe la transición de las unidades gestionadas al nuevo gestor central primario. Esta acción puede tardar algún tiempo en completarse. Utilizando un cliente SSH, conéctese al nuevo gestor central primario para ver el registro de resultados.
    a. Inicialice el servidor de archivos utilizando el mandato siguiente: `fileserver [ip_address] [duration]`
    b. En un navegador web, conéctese al nuevo gestor central primario.
    c. Consulte el archivo load_secondary_cm_sync_file.log para ver el progreso. El archivo se encuentra en el directorio gim-snif-guard-logs.
    d. Cuando vea la línea final Import CM sync info done, el proceso ha finalizado satisfactoriamente.
    e. En este punto, la interfaz de usuario se renueva y verá la página de inicio de sesión.
    f. Espere hasta que se complete la hora para que el proceso finalice, a medida que las unidades gestionadas comienzan la transición al nuevo gestor central primario.
18. Inicie sesión en la interfaz de usuario de Guardium y realice estos pasos:
    a. Verifique que las unidades gestionadas están ahora gestionadas por el nuevo gestor central primario.
    b. Verifique que todas las unidades gestionadas han realizado la transición, excepto para el gestor central primario antiguo.

Qué hacer a continuación

Después de actualizar correctamente el gestor central de copia de seguridad y haber realizado la transición de las unidades gestionadas, consulte Actualizar el gestor central primario de 32 bits antiguo.

Tema principal: Actualizar un entorno de 32 bits sin un gestor central de copia de seguridad
Tema siguiente: Actualizar el gestor central primario de 32 bits antiguo

Actualizar el gestor central primario de 32 bits antiguo

Cuando trabaje con un gestor central de copia de seguridad, siga estos procedimientos para actualizar el gestor central primario de 32 bits antiguo mediante un procedimiento de copia de seguridad, recompilación y restauración.

Antes de empezar

Una vez que el gestor central de copia de seguridad se haya convertido en el nuevo gestor central primario, puede actualizar el gestor central primario antiguo al último Guardium V10. Antes de actualizar el gestor central primario antiguo, revise y complete las tareas siguientes:

- Actualizar un entorno de 32 bits sin un gestor central de copia de seguridad
- Actualizar un gestor central de copia de seguridad de 32 bits

Procedimiento

1. Vuelva a configurar el gestor central primario antiguo utilizando el siguiente mandato de CLI: `delete unit type manager`. Antes de continuar, verifique que el gestor central primario antiguo sea ahora un agregador autónomo.
2. Realice una copia de seguridad del sistema del gestor central primario antiguo. Incluya tanto los datos como la configuración en la copia de seguridad.
3. Vuelva a crear el gestor central primario utilizando el procedimiento siguiente:
   a. Monte la imagen de ISO más reciente de Guardium V10.
   b. Seleccione un tipo de sistema a los cinco segundos de entrar en el instalador de Guardium. Cuando trabaje con un gestor central primario antiguo, seleccione Agregador .
   c. Permita que se complete la instalación y se reinicie el sistema.
4. Configure los parámetros de red. Inicie sesión en la CLI de Guardium y emita los mandatos siguientes:

```
store network interface ip
store network route defaultroute
store network resolver 1
store system hostname
store system domain
```

5. Inicie sesión en la interfaz de usuario de Guardium y verifique no haya licencias instaladas en el sistema.
   Consejo:
   - Si inicia sesión por primera vez, la contraseña predeterminada es `guardium`.
   - Si está trabajando con un sistema autónomo que finalmente se convertirá en una unidad gestionada, no es necesario instalar licencias.

   a. En la navegación principal de Guardium, verifique que solo estén visibles los elementos de navegación Bienvenido y Configuración.
   b. Vaya a Configurar > Herramientas y vistas > Licencia o pulse el icono para verificar que no hay ninguna licencia instalada en el sistema.
6. Si se han instalado la GPU V10 más reciente (si es más nueva que el ISO V10 más reciente) y los parches de mantenimiento en el gestor central de copia de seguridad antiguo antes de convertirlo en un gestor central primario, instale la misma GPU y los parches de mantenimiento en el gestor central primario antiguo.
7. Restaure los datos y la configuración en el gestor central.
   a. Emita el mandato siguiente de CLI de Guardium para importar los archivos: `import file`.
   b. Importe los datos y los archivos de configuración por separado.
   c. Realice la restauración de datos y de la configuración con el siguiente mandato de CLI: `restore db-from-prev-version`.
8. Establezca el secreto compartido en Configurar > Herramientas y vistas > Sistema.
9. Registre el gestor central primario antiguo (el sistema que acaba de actualizar) en el nuevo gestor central primario.
10. Defina un nuevo gestor central de copia de seguridad.
    a. Vaya a Gestionar > Gestión central > Gestión central en el nuevo gestor central primario.
    b. Seleccione el gestor central primario antiguo.
    c. Designe el gestor central primario antiguo como el nuevo gestor central de copia de seguridad.
    d. Espere a que se complete al menos una sincronización de copia de seguridad. La primera sincronización de copia de seguridad debe tener lugar en el plazo de una hora.
    e. Verifique que se haya creado el archivo cm_sync_file.tgz comprobando el registro de Agregación/Archivado en el nuevo gestor central primario.
11. Opcionalmente, vuelva a la configuración del entorno gestionado original, definiendo de nuevo el gestor central de copia de seguridad nuevo como gestor central primario.
    a. Responda `Sí` al mensaje: ¿Está seguro de que desea hacer que esta unidad sea el gestor central (CM) primario?
    b. Pulse Cerrar en el mensaje emergente Información. El icono de progreso se muestra en la página de la interfaz de usuario.
       Atención: La interfaz de usuario no estará disponible temporalmente durante el proceso de conversión. Una vez completado el proceso, la pantalla de inicio de sesión vuelve al estado normal.
12. Efectúe la transición de las unidades gestionadas al nuevo gestor central primario. Este proceso puede tardar algún tiempo en completarse. Utilizando un cliente SSH, conéctese al nuevo gestor central primario para ver el registro de resultados.
    a. Inicialice el servidor de archivos utilizando el mandato siguiente: `fileserver [ip_address] [duration]`
    b. En un navegador web, conéctese al nuevo gestor central primario.
    c. Consulte el archivo load_secondary_cm_sync_file.log para ver el progreso. El archivo se encuentra en el directorio gim-snif-guard-logs.
    d. Cuando vea la línea final Import CM sync info done, el proceso ha finalizado satisfactoriamente.
    e. En este punto, la interfaz de usuario se renueva y verá la página de inicio de sesión.
    f. Espere cinco minutos a que el proceso se complete, ya que las unidades gestionadas empiezan a realizar la transición al nuevo gestor central primario.
13. Vaya a Gestionar > Gestión central > Gestión central y verifique que todas las unidades gestionadas sean de color verde y estén ahora gestionadas por el gestor central primario original. El gestor central de copia de seguridad original no debe aparecer en la lista de unidades gestionadas, a menos que se haya vuelto a configurar como un gestor central de copia de seguridad.

Qué hacer a continuación

Ahora que ha actualizado el gestor central y el gestor central de copia de seguridad, Actualizar unidades gestionadas de 32 bits.
Tema principal: Actualizar un entorno de 32 bits sin un gestor central de copia de seguridad
Tema anterior: Actualizar un gestor central de copia de seguridad de 32 bits
Tema siguiente: Actualizar unidades gestionadas de 32 bits

Actualizar unidades gestionadas de 32 bits

Actualice las unidades gestionadas de 32 bits utilizando un procedimiento de copia de seguridad, recompilación y restauración.

Antes de empezar

Antes de actualizar las unidades gestionadas de 32 bits, revise y complete las tareas siguientes:

- Actualizar un entorno de 32 bits sin un gestor central de copia de seguridad
- Actualizar un gestor central de copia de seguridad de 32 bits
- Actualizar el gestor central primario de 32 bits antiguo

Importante: Debe actualizar el entorno al parche 600 V9 o posterior antes de actualizar a la V10 más reciente.

Procedimiento

1. Distribuya el parche más reciente de Comprobación de salud (p9997) para las unidades gestionadas y verifique que la instalación se ha realizado correctamente. Consulte la sección Instalación, distribución y supervisión de parches para obtener más información.
2. Realice copias de seguridad de todas las unidades gestionadas.
3. Vuelva a crear las unidades gestionadas utilizando el procedimiento siguiente:
   a. Monte la imagen de ISO más reciente de Guardium V10.
   b. Seleccione un tipo de sistema a los cinco segundos de entrar en el instalador de Guardium. Utilice la selección predeterminada Instalación estándar (no CM) con un tipo de unidad de recopilador autónomo.
   c. Permita que se complete la instalación y se reinicie el sistema.
4. Configure los parámetros de red. Inicie sesión en la CLI de Guardium y emita los mandatos siguientes:

```
store network interface ip
store network route defaultroute
store network resolver 1
store system hostname
store system domain
```

5. Inicie sesión en la interfaz de usuario de Guardium y verifique no haya licencias instaladas en el sistema.
   Consejo:
   - Si inicia sesión por primera vez, la contraseña predeterminada es `guardium`.
   - Si está trabajando con un sistema autónomo que finalmente se convertirá en una unidad gestionada, no es necesario instalar licencias.

   a. En la navegación principal de Guardium, verifique que solo estén visibles los elementos de navegación Bienvenido y Configuración.
   b. Vaya a Configurar > Herramientas y vistas > Licencia o pulse el icono para verificar que no hay ninguna licencia instalada en el sistema.
6. Restaure los datos y las configuraciones en las unidades gestionadas.
   Nota: Cuando se restaura una unidad gestionada desde una copia de seguridad, los diseños personalizados para dicha unidad gestionada se perderán si el gestor central está inactivo en el momento de la restauración.
   a. Emita el mandato siguiente de CLI de Guardium para importar los archivos: `import file`.
   b. Importe los datos y los archivos de configuración por separado.
   c. Realice la restauración de datos y de la configuración con el siguiente mandato de CLI: `restore db-from-prev-version`.
7. Cuando todas las unidades gestionadas se hayan actualizado correctamente, distribuya las licencias desde el gestor central a las unidades gestionadas.
   a. Inicie sesión en la interfaz de usuario del gestor central.
   b. Vaya a Gestión central > Gestionar > Gestión central y verifique que se listan las unidades gestionadas.
   c. Pulse el recuadro de selección Seleccionar todo para seleccionar todas las unidades gestionadas.
   d. Pulse el botón Renovar para distribuir las licencias a las unidades gestionadas.
   e. Espere hasta que se complete el proceso de renovación.
   f. Inicie sesión en la interfaz de usuario de las unidades gestionadas y vaya a Configuración > Herramientas y vistas > Licencia para verificar que se han instalado las licencias correctas. Cuando se hayan instalado las licencias correctas:
      - Las opciones de menú de navegación esperadas estarán disponibles en las unidades gestionadas.
      - Los informes sobre las unidades gestionadas serán funcionales.
      - Se podrá acceder a los informes a través de orígenes de datos remotos desde el gestor central.
8. Si se han instalado la GPU V10 más reciente (si es más nueva que ISO V10 más reciente) y los parches de mantenimiento en el gestor central, distribuye la GPU y los parches en las unidades gestionadas.
9. Si utiliza herramientas de VMware, debe volver a instalar estas herramientas después de completar la actualización. Para volver a instalar las Herramientas de VMware, inicie sesión en la CLI de Guardium, emita el siguiente mandato y siga las solicitudes: `setup vmware_tools install`.

Resultados

Ha completado correctamente una actualización de su entorno Guardium de 32 bits a la V10 más reciente utilizando un gestor central de copia de seguridad. Verifique la estabilidad del entorno Guardium.
Tema principal: Actualizar un entorno de 32 bits sin un gestor central de copia de seguridad
Tema anterior: Actualizar el gestor central primario de 32 bits antiguo

Actualizar un entorno de 64 bits con un gestor central de copia de seguridad

Actualice su entorno de Guardium de 64 bits utilizando un gestor central de copia de seguridad.

Antes de actualizar el entorno de Guardium de 64 bits, utilizando un gestor central de copia de seguridad, revise la siguiente lista de comprobación y complete cada elemento antes de intentar la actualización.

Importante: Antes de ejecutar `restore db` en un sistema de la V10, aplique los últimos parches de mantenimiento después de que se haya compilado su sistema para la V10. Si está utilizando un gestor central basado en recopiladores de 64 bits, el parche de actualización se encargará de actualizar y convertirá el sistema desde un gestor central basado en recopiladores en un gestor central basado en agregadores.

Lista de comprobación de actualización

- Identifique y registre todas las unidades gestionadas definidas en el entorno actual.
- Los sistemas actuales deben estar en el nivel de Guardium V9, parche 600, y tener una arquitectura de 64 bits.

- Descargue el último release de Guardium V9 o descárguelo más tarde desde Fix Central [opcional].
- Descargar el parche de actualización p10000
- Descargue los parches de mantenimiento más recientes desde Fix Central
- Descargue el último parche de comprobación de salud (p9997) desde Fix Central. Para obtener más información, consulte Notas del release del parche de comprobación de salud de Guardium.

1. Actualizar un gestor central de copia de seguridad de 64 bits
   Cuando actualice el entorno de Guardium de 64 bits, siga estos pasos para ejecutar el parche de comprobación de estado y actualizar un gestor central de copia de seguridad mediante un procedimiento de copia de seguridad, reconstrucción y restauración.
2. Actualizar el gestor central primario de 64 bits antiguo
   Cuando trabaje con un gestor central de copia de seguridad, siga estos procedimientos para actualizar el gestor central primario de 64 bits antiguo mediante un parche de actualización.
3. Actualizar unidades gestionadas de 64 bits
   Actualice las unidades gestionadas de 64 bits utilizando un parche de actualización.

Tema principal: Actualización del sistema Guardium
Conceptos relacionados:
Planificación de una actualización

Actualizar un gestor central de copia de seguridad de 64 bits

Cuando actualice el entorno de Guardium de 64 bits, siga estos pasos para ejecutar el parche de comprobación de estado y actualizar un gestor central de copia de seguridad mediante un procedimiento de copia de seguridad, reconstrucción y restauración.

Antes de empezar

Complete la lista de comprobación de la actualización de la sección Actualizar un entorno de 64 bits con un gestor central de copia de seguridad.

Procedimiento

1. Actualice el sistema a la versión 9, parche 600 o posterior.
2. Establezca la hora en el huso horario local y sincronice la hora en todos los sistemas Guardium utilizando un servidor NTP.
3. Descargue e instale el parche de comprobación de estado más reciente (p9997) y verifique que la instalación se ha realizado correctamente. Consulte el apartado Instalación, distribución y supervisión de parches para obtener instrucciones.
   Importante: Necesitará instalar el parche de comprobación de estado más reciente (p9997) en el gestor central primario y en el gestor central de copia de seguridad candidato antes de designar un gestor central de copia de seguridad.
4. Defina un nuevo gestor central de copia de seguridad.
   a. Vaya a la página Gestión central en el gestor central primario.
   b. Seleccione un agregador gestionado.
   c. Verifique que el gestor central primario y el gestor central de copia de seguridad candidato tengan instalados los mismos parches.
   d. Designe el agregador como un gestor central de copia de seguridad.
   e. Verifique que el archivo cm_sync_file.tgz se haya creado, comprobando el Registro de agregación/archivado en el nuevo gestor central.
5. Realice una copia de seguridad del sistema del gestor central de copia de seguridad y verifique que se ha realizado correctamente.
   a. Vaya a Gestionar > Gestión de datos > Copia de seguridad del sistema.
   b. Configure el protocolo en función de sus preferencias y rellene todos los campos.
   c. Asegúrese de que realiza una copia de seguridad de la configuración y los datos.
   Importante: Cree al menos una copia de seguridad válida antes de empezar el procedimiento de actualización.
6. Instale p10000 en el gestor central y supervise su instalación.
   Importante: Una vez realizada la instalación del parche, el proceso de actualización se inicia automáticamente y se reinicia el sistema. No reinicie manualmente el sistema.
7. Permita que finalice la instalación del sistema operativo.
   - El tiempo de instalación depende de la cantidad de datos implicados, así como de la configuración y las especificaciones del sistema
   - Una vez completada la instalación del sistema operativo, el sistema rearranca por primera vez en Guardium V10 más reciente.
     Atención: Después de instalar correctamente la Versión 10 más reciente, el primer arranque del sistema va seguido de:
     - Configuración de red, migración de datos de base de datos, inicio de base de datos.
     - Actualización de licencia, actualización de PSML y ajuste del idioma.
     - Reinicio de base de datos, migración de certificados y claves, migración de contraseña y limpieza de archivos.
8. Confirme que la actualización de CM de copia de seguridad se ha completado correctamente utilizando los pasos siguientes
   a. Inicie sesión en la CLI.
   b. Emita el mandato de CLI siguiente: show upgrade-status
   c. Verifique que la última línea de la salida sea: 5.0:INFO:Migration Complete
   d. Emita el mandato de CLI siguiente: show system patch install
   e. Verifique que el estado de p10000 es el siguiente: Fase 5: Migración completada
9. Instale los parches de mantenimiento más recientes en el gestor central y verifique que se han instalado correctamente.
10. Verifique que el gestor central primaria todavía ve el gestor central de copia de seguridad actualizado.
    Importante: El gestor central de copia de seguridad (que ahora ejecuta el último Guardium V10) puede mostrar una luz de estado de color rojo. Esto sucede cuando el gestor central envía una señal V9 a un sistema V10 y falla, y puede seguir promocionando el servidor siempre que el archivo de sincronización del gestor central esté presente en el gestor central de copia de seguridad. No intente realizar una renovación.
11. Verifique que el archivo cm_sync_file.tgz haya completado al menos dos transferencias correctas desde el gestor central primario al gestor central de copia de seguridad, comprobando el Registro de agregación/archivado en el gestor central primario. Las transferencias deben realizarse a intervalos de 30 minutos.
12. Convierta el gestor central de copia de seguridad en el gestor central primario. Es posible que se muestre el siguiente mensaje después de iniciar sesión en el gestor central de copia de seguridad:

    ```
    La versión del gestor central es inferior a la versión de esta unidad gestionada. La funcionalidad está limitada hasta que se corrija la discordancia de versiones.
    ```

    a. Vaya a Configurar > Gestión de datos.
    b. Pulse Convertir en CM primario. Si no ve esta opción, verifique que cm_sync_file se haya transferido correctamente.
    c. Responda Sí al mensaje: ¿Está seguro de que desea hacer que esta unidad sea el gestor central (CM) primario?

d. Pulse Cerrar en el mensaje emergente: El cambio tardará unos minutos y requerirá reiniciar la interfaz gráfica de usuario. Se cerrará la sesión cuando se realice el reinicio de la GUI. El icono de progreso se muestra en la página de la interfaz de usuario.

Nota: Durante el proceso de conversión, la interfaz de usuario de Guardium no está disponible temporalmente. Una vez completado el proceso, la pantalla de inicio de sesión vuelve al estado normal.

13. Efectúe la transición de las unidades gestionadas al nuevo gestor central primario. Esta acción puede tardar algún tiempo en completarse. Utilizando un cliente SSH, conéctese al nuevo gestor central primario para ver el registro de resultados.
    a. Inicialice el servidor de archivos utilizando el mandato siguiente: `fileserver [ip_address] [duration]`
    b. En un navegador web, conéctese al nuevo gestor central primario.
    c. Consulte el archivo load_secondary_cm_sync_file.log para ver el progreso. El archivo se encuentra en el directorio gim-snif-guard-logs.
    d. Cuando vea la línea final Import CM sync info done, el proceso ha finalizado satisfactoriamente.
    e. En este punto, la interfaz de usuario se renueva y verá la página de inicio de sesión.
    f. Espere hasta que se complete la hora para que el proceso finalice, a medida que las unidades gestionadas comienzan la transición al nuevo gestor central primario.
14. Inicie sesión en la interfaz de usuario de Guardium y acepte los acuerdos de licencia para habilitar las características del producto.
    a. Vaya a Configurar > Herramientas y vistas > Licencia.
    b. Acepte el acuerdo de licencia base.
    c. Acepte todos los acuerdos de licencia adicionales.

    Nota: Omitir este paso evita que las funciones de Guardium estén habilitadas.
15. Vaya a la página Gestión central y asegúrese de que ahora el gestor central primario gestiona las unidades gestionadas. El gestor central de copia de seguridad antiguo no debe aparecer en la lista de unidades gestionadas.

Qué hacer a continuación

Después de actualizar correctamente el gestor central de copia de seguridad y haber realizado la transición de las unidades gestionadas, consulte Actualizar el gestor central primario de 64 bits antiguo.

Tema principal: Actualizar un entorno de 64 bits con un gestor central de copia de seguridad

Tema siguiente: Actualizar el gestor central primario de 64 bits antiguo

Actualizar el gestor central primario de 64 bits antiguo

Cuando trabaje con un gestor central de copia de seguridad, siga estos procedimientos para actualizar el gestor central primario de 64 bits antiguo mediante un parche de actualización.

Antes de empezar

Cuando el gestor central de copia de seguridad se haya convertido en el nuevo gestor central primario, puede migrar el gestor central primario antiguo al último Guardium V10. Antes de actualizar el gestor central primario antiguo, revise y complete las tareas siguientes:

- Actualizar un entorno de 64 bits con un gestor central de copia de seguridad
- Actualizar un gestor central de copia de seguridad de 64 bits

Procedimiento

1. Vuelva a configurar el gestor central primario antiguo utilizando el siguiente mandato de CLI: `delete unit type manager`. Antes de continuar, verifique que el gestor central primario antiguo sea ahora un agregador autónomo.
2. Realice una copia de seguridad del sistema del gestor central primario antiguo. Incluya tanto los datos como la configuración en la copia de seguridad.
3. Actualice el gestor central primario antiguo utilizando el parche de actualización p10000 y supervise la instalación del parche. Lea la sección Instalación, distribución y supervisión de parches para obtener más información.

   Atención: Una vez realizada la instalación del parche, el proceso de actualización se inicia automáticamente y se reinicia el sistema. No reinicie manualmente el sistema.

   El tiempo necesario para la actualización depende de la cantidad de datos implicados, así como de la configuración y las especificaciones del sistema. Cuando se completa la actualización y el sistema se reinicia, el primer arranque del sistema actualizado va seguido de:
   - Configuración de red, migración de datos de base de datos, inicio de base de datos.
   - Actualización de licencia, actualización de PSML y ajuste del idioma.
   - Reinicio de base de datos, migración de certificados y claves, migración de contraseña y limpieza de archivos.

   Durante este proceso, no podrá iniciar la sesión en unidades gestionadas actualizadas hasta que finalice la migración de la base de datos.
4. Verifique que el proceso de actualización se haya completado correctamente en el gestor central primario antiguo.
   a. Inicie sesión en la CLI de Guardium del sistema que se está actualizando. Si la CLI entra en modalidad de recuperación, la actualización aún está en curso.
   b. Emita el mandato de CLI siguiente: `show upgrade-status`. Este mandato también se puede emitir desde la modalidad de recuperación de CLI.
   c. Verifique que la última línea de la salida sea: `5.0:INFO:Migration Complete`.
   d. Si está en modalidad de recuperación de CLI, salga de la CLI y vuelva a iniciar sesión para entrar en la modalidad de CLI.
   e. Emita el mandato de CLI siguiente: `show system patch install`.
      Atención: El mandato `show system patch install` no devuelve resultados hasta que se completa la actualización, después del primer reinicio.
   f. Verifique que el estado de instalación del parche de actualización sea: `Fase 5: Migración completada`.
5. Si se han instalado la GPU V10 más reciente (si es más nueva que el ISO V10 más reciente) y los parches de mantenimiento en el gestor central de copia de seguridad antiguo antes de convertirlo en un gestor central primario, instale la misma GPU y los parches de mantenimiento en el gestor central primario antiguo.
6. Establezca el secreto compartido en Configurar > Herramientas y vistas > Sistema.
7. Registre el gestor central primario antiguo (el sistema que acaba de actualizar) en el nuevo gestor central primario.
8. Defina un nuevo gestor central de copia de seguridad.
   a. Vaya a Gestionar > Gestión central > Gestión central en el nuevo gestor central primario.
   b. Seleccione el gestor central primario antiguo.
   c. Designe el gestor central primario antiguo como el nuevo gestor central de copia de seguridad.
   d. Espere a que se complete al menos una sincronización de copia de seguridad. La primera sincronización de copia de seguridad debe tener lugar en el plazo de una hora.
   e. Verifique que se haya creado el archivo cm_sync_file.tgz comprobando el registro de Agregación/Archivado en el nuevo gestor central primario.
9. Opcionalmente, vuelva a la configuración del entorno gestionado original, definiendo de nuevo el gestor central de copia de seguridad nuevo como gestor central primario.
   a. Responda `Sí` al mensaje: ¿Está seguro de que desea hacer que esta unidad sea el gestor central (CM) primario?
   b. Pulse Cerrar en el mensaje emergente Información. El icono de progreso se muestra en la página de la interfaz de usuario.

Atención: La interfaz de usuario no estará disponible temporalmente durante el proceso de conversión. Una vez completado el proceso, la pantalla de inicio de sesión vuelve al estado normal.

10. Efectúe la transición de las unidades gestionadas al nuevo gestor central primario. Este proceso puede tardar algún tiempo en completarse. Utilizando un cliente SSH, conéctese al nuevo gestor central primario para ver el registro de resultados.
    a. Inicialice el servidor de archivos utilizando el mandato siguiente: `fileserver [ip_address] [duration]`
    b. En un navegador web, conéctese al nuevo gestor central primario.
    c. Consulte el archivo load_secondary_cm_sync_file.log para ver el progreso. El archivo se encuentra en el directorio gim-snif-guard-logs.
    d. Cuando vea la línea final Import CM sync info done, el proceso ha finalizado satisfactoriamente.
    e. En este punto, la interfaz de usuario se renueva y verá la página de inicio de sesión.
    f. Espere cinco minutos a que el proceso se complete, ya que las unidades gestionadas empiezan a realizar la transición al nuevo gestor central primario.
11. Vaya a Gestionar > Gestión central > Gestión central y verifique que todas las unidades gestionadas sean de color verde y estén ahora gestionadas por el gestor central primario original. El gestor central de copia de seguridad original no debe aparecer en la lista de unidades gestionadas, a menos que se haya vuelto a configurar como un gestor central de copia de seguridad.

Qué hacer a continuación

Ahora que ha actualizado el gestor central y el gestor central de copia de seguridad, Actualizar unidades gestionadas de 64 bits.
Tema principal: Actualizar un entorno de 64 bits con un gestor central de copia de seguridad
Tema anterior: Actualizar un gestor central de copia de seguridad de 64 bits
Tema siguiente: Actualizar unidades gestionadas de 64 bits

Actualizar unidades gestionadas de 64 bits

Actualice las unidades gestionadas de 64 bits utilizando un parche de actualización.

Antes de empezar

Antes de actualizar las unidades gestionadas de 64 bits utilizando un parche de mantenimiento, revise y complete las tareas siguientes:

- Actualizar un entorno de 64 bits con un gestor central de copia de seguridad
- Actualizar un gestor central de copia de seguridad de 64 bits
- Actualizar el gestor central primario de 64 bits antiguo

Importante: Debe actualizar el entorno al parche 600 V9 o posterior antes de actualizar a la V10 más reciente.

Procedimiento

1. Distribuya el parche más reciente de Comprobación de salud (p9997) para las unidades gestionadas y verifique que la instalación se ha realizado correctamente. Consulte la sección Instalación, distribución y supervisión de parches para obtener más información.
2. Realice copias de seguridad de todas las unidades gestionadas.
3. Transfiera el parche de actualización de p10000 al gestor central y haga que esté disponible para las unidades gestionadas.
    a. Transfiera el parche de actualización al gestor central. Lea la sección Instalación, distribución y supervisión de parches para obtener más información.
    b. Haga que el parche de actualización esté disponible para las unidades gestionadas emitiendo el mandato de CLI siguiente desde el gestor central: `show system patch available`.
4. Distribuya el parche de actualización de p10000 a todas las unidades gestionadas y supervise la instalación del parche. Lea la sección Instalación, distribución y supervisión de parches para obtener más información.
   Atención: Una vez realizada la instalación del parche, el proceso de actualización se inicia automáticamente y se reinicia el sistema. No reinicie manualmente el sistema.
   El tiempo necesario para la actualización depende de la cantidad de datos implicados, así como de la configuración y las especificaciones del sistema. Cuando se completa la actualización y el sistema se reinicia, el primer arranque del sistema actualizado va seguido de:
    - Configuración de red, migración de datos de base de datos, inicio de base de datos.
    - Actualización de licencia, actualización de PSML y ajuste del idioma.
    - Reinicio de base de datos, migración de certificados y claves, migración de contraseña y limpieza de archivos.

   Durante este proceso, no podrá iniciar la sesión en unidades gestionadas actualizadas hasta que finalice la migración de la base de datos.
5. Verifique que el proceso de actualización se haya completado correctamente en cada unidad gestionada.
    a. Inicie sesión en la CLI de Guardium del sistema que se está actualizando. Si la CLI entra en modalidad de recuperación, la actualización aún está en curso.
    b. Emita el mandato de CLI siguiente: `show upgrade-status`. Este mandato también se puede emitir desde la modalidad de recuperación de CLI.
    c. Verifique que la última línea de la salida sea: `5.0:INFO:Migration Complete`.
    d. Si está en modalidad de recuperación de CLI, salga de la CLI y vuelva a iniciar sesión para entrar en la modalidad de CLI.
    e. Emita el mandato de CLI siguiente: `show system patch install`.
       Atención: El mandato `show system patch install` no devuelve resultados hasta que se completa la actualización, después del primer reinicio.
    f. Verifique que el estado de instalación del parche de actualización sea: `Fase 5: Migración completada`.
6. Cuando todas las unidades gestionadas se hayan actualizado correctamente, distribuya las licencias desde el gestor central a las unidades gestionadas.
    a. Inicie sesión en la interfaz de usuario del gestor central.
    b. Vaya a Gestión central > Gestionar > Gestión central y verifique que se listan las unidades gestionadas.
    c. Pulse el recuadro de selección Seleccionar todo para seleccionar todas las unidades gestionadas.
    d. Pulse el botón Renovar para distribuir las licencias a las unidades gestionadas.
    e. Espere hasta que se complete el proceso de renovación.
    f. Inicie sesión en la interfaz de usuario de las unidades gestionadas y vaya a Configuración > Herramientas y vistas > Licencia para verificar que se han instalado las licencias correctas. Cuando se hayan instalado las licencias correctas:
        - Las opciones de menú de navegación esperadas estarán disponibles en las unidades gestionadas.
        - Los informes sobre las unidades gestionadas serán funcionales.
        - Se podrá acceder a los informes a través de orígenes de datos remotos desde el gestor central.
7. Si se han instalado la GPU V10 más reciente (si es más nueva que ISO V10 más reciente) y los parches de mantenimiento en el gestor central, distribuye la GPU y los parches en las unidades gestionadas.
8. Si utiliza herramientas de VMware, debe volver a instalar estas herramientas después de completar la actualización. Para volver a instalar las Herramientas de VMware, inicie sesión en la CLI de Guardium, emita el siguiente mandato y siga las solicitudes: `setup vmware_tools install`.

Resultados

Ha completado correctamente una actualización de su entorno Guardium de 64 bits a la V10 más reciente utilizando un gestor central de copia de seguridad. Verifique la estabilidad del entorno Guardium.
Tema principal: Actualizar un entorno de 64 bits con un gestor central de copia de seguridad
Tema anterior: Actualizar el gestor central primario de 64 bits antiguo

CLI y API

La interfaz de línea de mandatos (CLI) de Guardium es una herramienta administrativa que permite la configuración, resolución de problemas y gestión del sistema Guardium. La interfaz de programación de aplicaciones (API) de Guardium proporciona acceso a muchas funciones de Guardium desde la línea de mandatos.

- Visión general de CLI
  La interfaz de línea de mandatos (CLI) de Guardium es una herramienta administrativa que permite la configuración, resolución de problemas y gestión del sistema Guardium.
- Referencia de GuardAPI
  GuardAPI proporciona acceso a las funciones de Guardium desde la línea de mandatos.

Visión general de CLI

La interfaz de línea de mandatos (CLI) de Guardium es una herramienta administrativa que permite la configuración, resolución de problemas y gestión del sistema Guardium.

Convenios de la documentación

Todos los ejemplos de mandatos de CLI se escriben en texto courier (por ejemplo, show system clock).

Para ilustrar las reglas de sintaxis, algunas descripciones de mandatos utilizan delimitadores de dependencia. Dichos delimitadores indican qué argumentos de mandato son obligatorios y en qué contexto. Cada descripción de sintaxis muestra las dependencias entre los argumentos del mandato utilizando caracteres especiales:

- Los símbolos < y > indican un argumento necesario.
- Los símbolos [y] indican un argumento opcional.
- El símbolo | (barra vertical) separa las opciones alternativas cuando solo se puede seleccionar una. Por ejemplo:

```
store full-bypass <ON | OFF>
```

Uso de mandatos de CLI

- Los mandatos y las palabras clave se pueden abreviar especificando suficientes caracteres para que los mandatos no sean ambiguos. Por ejemplo, se puede abreviar show como sho.
- La mayor parte de los mandatos de CLI de Guardium constan de una palabra de mandato seguida de uno o varios argumentos. El argumento puede ser una palabra clave o una palabra clave seguida de un valor de variable, por ejemplo una dirección IP, una máscara de subred, fecha, etc.
- Los mandatos y las palabras clave no distinguen entre mayúsculas y minúsculas, pero los nombres de elemento sí distinguen.
- Para visualizar la sintaxis de los mandatos y las opciones de uso, escriba un signo de interrogación (?) como un argumento, después de la palabra del mandato.
- Encierre las palabras o frases entre comillas para definir con precisión los términos de búsqueda.

Acceso a la CLI

Un administrador puede acceder a la CLI mediante:

- Una consola de PC conectada físicamente o un terminal en serie O
- Una conexión de red utilizando un cliente SSH

Acceso a la consola física

El acceso interactivo al dispositivo Guardium se realiza a través del puerto serie o de la consola del sistema.

Teclado y pantalla de PC: Se puede conectar una pantalla de vídeo de PC al conector de vídeo del panel frontal o al conector de vídeo de la parte posterior del dispositivo.

Se puede conectar un teclado de PC con un conector de estilo PS/2 al conector PS/2 de la parte posterior del dispositivo. De forma alternativa, se puede conectar un teclado USB a los conectores USB situados en la parte frontal o posterior del dispositivo.

Acceso al puerto serie: Utilizando un cable de módem nulo, conecte un terminal u otro sistema al puerto serie de 9 patillas de la parte posterior del dispositivo. El terminal o un emulador de terminal del sistema conectado, se debe establecer para que se comunique como 19200-N-1 (19200 baudios, sin paridad, 1 bit de detención).

Cuando el terminal se conecta al puerto serie, o cuando el teclado y la pantalla están conectados a la consola, se muestra un indicador de inicio de sesión. Escriba cli como nombre de usuario y continúe con el inicio de sesión en CLI.

Acceso a SSH de red

El acceso remoto a la CLI está disponible en la dirección IP o el nombre de dominio de gestión, utilizando un cliente SSH. Los clientes SSH están disponibles libremente o comercialmente para la mayoría de las plataformas de servidor. Un mandato de conexión SSH de Unix para iniciar sesión como usuario de CLI puede ser similar al siguiente:

```
ssh -l cli 192.168.2.16
```

Es posible que el cliente SSH le solicite que acepte la huella dactilar criptográfica del dispositivo Guardium. Acepte la huella dactilar para continuar en la solicitud de contraseña.

Nota: Si, después de la primera conexión, se le vuelve a solicitar la huella dactilar, es posible que alguien esté intentado inducirle a iniciar sesión en la máquina incorrecta.

Inicio de sesión de CLI

Acceda a CLI mediante la cuenta admin de CLI, cli, o mediante una de las cinco cuentas de CLI (guardcli1,...,guardcli5). Las cinco cuentas de CLI (guardcli1,...,guardcli5) ayudan a separar las responsabilidades administrativas.

El acceso a GuardAPI, que es un conjunto de mandatos de CLI para ayudar en la automatización de tareas repetitiva, requiere que el gestor de acceso creer un usuario (nombre de usuario de GUI/guiuser) y proporcione a estas cuentas el rol admin o cli. Para un inicio de sesión correcto en CLI para utilizar GuardAPI es necesario iniciar sesión con una de las cinco cuentas de CLI (guardcli1,...,guardcli5) y un inicio de sesión adicional con guiuser, emitiendo el mandato 'set guiuser'. Para obtener más información, consulte la sección Visión general de la Referencia de GuardAPI o Establecer la autenticación de guiuser.

Reforzar contraseñas

Para cumplir con los diferentes requisitos de auditoría y conformidad, se aplican los siguientes refuerzos de contraseñas para las cuentas de CLI:

- Para la cuenta cli, utilice la contraseña cli proporcionada o asegúrese de que establece una contraseña fuerte para proteger esta cuenta. Si acaba de volver a crear el sistema desde un DVD de instalación, el usuario cli de Guardium tiene una contraseña predeterminada de guardium. Debe cambiar esta contraseña inmediatamente.
- Se aplica un periodo de caducidad a la cuenta CLI y a las cinco cuentas CLI con un valor predeterminado de 90 días. Cuando caduca una contraseña, se invoca el cambio obligatorio de contraseña durante el proceso de inicio de sesión.
- Las contraseñas deben tener un mínimo de ocho caracteres.
- Las contraseñas deben contener al menos un carácter de tres de las cuatro clases siguientes
  - Cualquier letra en mayúsculas
  - Cualquier letra en minúsculas
  - Cualquier número (0,1,2,...)
  - Cualquier carácter no alfanumérico (especial)
- Una vez otorgado el acceso utilizando un nombre de usuario de GUI separado (guiuser), el seguimiento de auditoría de CLI muestra el par de CLI_USER+GUI_USER que se ha utilizado para el inicio de sesión.
- Los usuarios de CLI no se pueden autenticar a través de LDAP, ya que se consideran cuentas administrativas y pueden iniciar sesión independientemente de la conexión con un servidor LDAP.

Mandatos de CLI limitados durante el mantenimiento de la base de datos interna

La CLI tiene tres conjuntos de mandatos: Mandatos generales, mandatos de soporte especializados y mandatos de recuperación. Los mandatos de soporte los utiliza el soporte técnico para analizar el sistema. Los mandatos de recuperación son para la recuperación del sistema cuando la base de datos no está activa.

El inicio de sesión de CLI es:

```
Welcome to CLI - your last login was <date>
```

El mensaje de bienvenida añadirá más información si la base de datos interna está inactiva, debido a mantenimiento o durante una actualización.

Si este es el caso, el número de mandatos de CLI disponibles será limitado.

```
The internal database on the appliance is currently down and CLI will be working
in "recovery mode";  only a limited set of commands will be available.
```

Los mandatos de CLI disponibles para su uso durante la modalidad de recuperación son los siguientes:

```
support reset-password root
restart mysql
restart stopped_services
restart system
restore pre-patch-backup
restore system
```

- Mandatos de CLI del agregador
  Esta sección lista los mandatos de CLI del agregador.
- Mandatos de CLI del alertador
  Esta sección lista los mandatos de CLI del alertador.
- Mandatos de CLI de certificados
  Utilice los mandatos de certificado para crear una solicitud de firma de certificado (CSR), y para instalar certificados de servidor, CA (entidad emisora de certificados) o certificados de vía de acceso de confianza en el sistema Guardium.
- Mandatos de CLI de configuración y control
  Utilice los siguientes mandatos de CLI para configuración y control.
- Mandato de CLI diag
  Utilice estos mandatos de CLI para acceder a programas de utilidad de resolución de problemas y mantenimiento a través de diag.
- Mandatos de CLI de manejo de archivos
  Utilice estos mandatos para la copia de seguridad y restauración de la información del sistema. Muchas de estas tareas se pueden realizar desde la interfaz de usuario de Guardium.
- Mandatos de CLI del motor de inspección
  Utilice estos mandatos de CLI para configurar el motor de inspección.
- Mandatos de CLI del panel de control de investigación
  Utilice estos mandatos de CLI para configurar el panel de control de investigación.
- Mandatos de CLI de configuración de red
  Utilice los mandatos de CLI de configuración de red para establecer dirección IP, manejar el acoplamiento/migración tras error, manejar las funciones secundarios y restablecer las redes.
- Mandatos de CLI de soporte
  Los siguientes mandatos de CLI solo se han de utilizar siguiendo las instrucciones del servicio de soporte técnico.
- Mandatos de CLI sistema
  Utilice estos mandatos de CLI para configurar los valores del sistema.
- Mandatos de CLI de cuenta de usuario, contraseña y autenticación
  Utilice estos mandatos de CLI para configurar las cuentas de usuario, las contraseñas y la autenticación.

Tema principal: CLI y API
Información relacionada:
Gestión y configuración avanzadas del sistema Guardium (vídeo)

Mandatos de CLI del agregador

Esta sección lista los mandatos de CLI del agregador.

archivo de claves de copia de seguridad del agregador

Utilice este mandato para realizar una copia de seguridad del archivo de clave secreta compartida en la ubicación especificada.

Sintaxis

aggregator backup keys file <user@host:/path/filename>

Parámetros

user@host:/path/filename. Para la operación de transferencia de archivos, especifica un usuario, host y nombre de vía de acceso completa del archivo de claves de copia de seguridad. El usuario que especifique debe tener autorización de escritura en el directorio especificado.

Nota: Para obtener más información sobre cómo utilizar el secreto compartido, consulte la sección Secreto compartido del sistema.

aggregator clean shared-secret

Establece el valor del secreto compartido del sistema en nulo. Todos los archivos que se hayan archivado o exportado desde una unidad y que tengan un secreto compartido nulo se pueden restaurar o importar únicamente en los sistemas en los que el secreto compartido sea nulo.

Sintaxis

aggregator clean shared-secret

Nota: Para obtener más información sobre cómo utilizar el secreto compartido, consulte la sección Secreto compartido del sistema.

aggregator debug

Inicia o detiene la escritura o información de depuración relacionada con las actividades de agregación. Utilice estos mandatos solo cuando se le indique el servicio de soporte de Guardium y asegúrese de emitir el mandato stop después de haber recopilado suficiente información.

Nota: La modalidad de depuración caduca automáticamente transcurridos 7 días.

Sintaxis

aggregator debug <start | stop>

aggregator list failed imports

Cuando falla una operación de importación debido a una falta de coincidencia del secreto compartido, el archivo afectado se traslada desde el directorio /var/importdir al directorio /var/dump, y se cambia su nombre añadiendo el sufijo .decrypt_failed al nombre de archivo original. Utilice este mandato para listar todos estos archivos

Sintaxis

aggregator list failed imports

aggregator recover failed import

Utilice este mandato para mover y cambiar el nombre de los archivos de importación anómalos, antes de volver a intentar una operación de importación o restauración. Los archivos de importación anómalos se almacenan en el directorio /var/dump, con el sufijo .decrypt_failed. Antes de volver a intentar una operación de importación o restauración, se debe cambiar el nombre de estos archivos (eliminando el sufijo .decrypt_failed) y se deben trasladar los archivos al directorio /var/importdir.

Sintaxis

aggregator recover failed import <all | filename>

Parámetros

Utilice la opción all para trasladar todos los archivos del directorio /var/dump que terminan con el sufijo .decrypt_failed, o utilice la opción filename para identificar un único archivo para trasladarlo.

Nota: Después de mover los archivos anómalos, pero antes de que se ejecute una operación de importación o exportación, asegúrese de que el secreto compartido del sistema coincida con el secreto compartido utilizado para el archivo exportado o archivado.

aggregator restore keys file

Utilice este mandato para restaurar una copia de seguridad del archivo de claves secretas compartidas desde la ubicación especificada.

Sintaxis

aggregator restore keys file <user@host:/path/filename>

Parámetros

user@host:/path/filename. Para la operación de transferencia de archivos, especifica un usuario, host y nombre de vía de acceso completa del archivo de claves de copia de seguridad.

Nota: Para obtener más información sobre cómo utilizar el secreto compartido, consulte la sección Secreto compartido del sistema.

store aggregator drop_ad_hoc_audit_db

Informes de procesos de auditoría en el agregador - Crea bases de datos ad-hoc para cada una de sus tareas que solo incluirán los días relevantes para dicha tarea. Estas bases de datos ad-hoc se pueden guardar durante 14 días (para análisis) o suprimirse inmediatamente después de su uso. El mandato de CLI define la política de depuración de bases de datos ad-hoc. Las opciones son 0 o 1 (0 - conservar durante 14 días o 1 - suprimir después de utilizar).

Sintaxis

store aggregator drop_ad_hoc_audit_db [1|0]

Drop ad-hoc merge databases? 0

show aggregator drop_ad_hoc_audit_db

store aggregator orphan_cleanup_flag

Utilice este mandato CLI para ejecutar de forma habitual la limpieza de huérfanos estáticos en un agregador.

Utilice este mandato de CLI para limpiar huérfanos en agregadores planificados para que se ejecuten en datos con una antigüedad superior a 3 días al final de una depuración.

Este proceso lo inicia el usuario con este mandato de CLI, de modo que si la base de datos es grande, el usuario tendrá en cuenta el periodo de tiempo que puede durar el proceso.

Esto cubre todos los datos del agregador, pero se ejecutará todo en una base de datos separada.

Nota: En un recopilador, la limpieza de huérfanos no varía. Se ejecuta con las tácticas de limpieza pequeña y se invoca antes de exportar o archivar.

show aggregator orphan_cleanup_flag Muestra small, large o analyze.

store aggregator orphan_cleanup_flag

store aggregator orphan_cleanup_flag <flag>, donde flag es una de estas palabras: < small large analyze >

Estos mandatos solo se aplican al agregador.

Si se establece en uno de los valores small, large o analyze, se invoca el script de limpieza de huérfanos después de cada proceso de ejecución o depuración.

La limpieza de huérfanos en un agregador no elimina los registros de huérfanos de los últimos 3 días, pero elimina todos lo huérfanos de más de 3 días.

Si se especifica small, el proceso no interfiere con los procesos de auditoría que pueden iniciarse después de que se haya completado la fusión.

Si se especifica large, el proceso se ejecuta más rápido cuando existe un número elevado de huérfanos pero su ejecución puede interferir con los procesos de auditoría. Cuando se especifica large, los procesos de auditoría no se inician hasta que se ha completado la limpieza de huérfanos.

Si se especifica analyze, en primer lugar, el proceso evalúa el número de huérfanos y utiliza las mismas tácticas que en large, si hay más de un 20% huérfanos. Cuando se especifica analyze, los procesos de auditoría no se inician hasta que se ha completado la limpieza de huérfanos.

Sintaxis

store aggregator orphan_cleanup_flag [small | large | analyze]

Mandato show

show aggregator orphan_cleanup_flag

store archive_static_table

Utilice este mandato de CLI para desactivar/activar la tabla estática de archivado

USO: store archive_static_table <state>,

donde state es on/off.

Mandato show

show archive_static_table

store next_export_static

El software de agregación diferencia entre dos tipos de tablas:

- tablas estáticas: Crecen lentamente con el tiempo y los datos de estas tablas no dependen del tiempo (GDM_OBJECT, GDM_FIELD, GDM_SENTENCE, GDM_CONSTRUCT, etc.).
- tablas dinámicas: Crecen rápidamente con el tiempo y los datos dependen del tiempo (GDM_CONSTRUCT_INSTANCE, GDM_SESSION, GDM_CONSTRUCT_TEXT etc.).

Como se ha indicado anteriormente, los datos de las tablas estáticas no dependen del tiempo . Los datos de las tablas dinámicas que dependen del tiempo están enlazados con datos estáticos. Dado que el tamaño de las tablas estáticas puede aumentar mucho, el proceso de exportación o archivado no archiva los datos estáticos completos cada día. Sino que archiva los datos estáticos completos la primera vez que se ejecuta y, a continuación, el primer día de cada mes, y en cualquier día además del primer día del mes, solo archiva los datos estáticos que se han modificado durante ese día. Por este motivo, cuando se restauran los datos de cualquier día, también es necesario que se restauren el primer día del mes. Esto garantiza que los datos estáticos completos estén presentes y que no estén dañadas las referencias.

Utilice el mandato de CLI, store next_export_static, para establecer un distintivo, de modo que la exportación contenga los datos estáticos completos.

Sintaxis

store next_export_static [ON | OFF]

Mandato show

show next_export_static

store last_used

Utilice este mandato de CLI durante la depuración y agregación.

Sintaxis

store last_used [size | interval | logging]

Mandato show

show last_used [size | interval | logging]

LAST_USED SIZE - Entero. El valor predeterminado es 50

LAST_USED INTERVAL - Enero. El valor predeterminado es 60 (minutos)

LAST_USED LOGGING - Entero

Todas las tablas - 1

Solo GDM_Object - 2

Ninguna - 0 (Valor predeterminado)

store aggregator static_data

store aggregator static_data [TIMESTAMP | LAST_USED_FOR_OBJECT_ONLY | LAST_USED]

Nota: Establezca el mandato de CLI last_used logging, antes de utilizar este mandato.

Cuando Sniffer actualiza la columna LAST_USED en las tablas estáticas, se puede hacer referencia a esta columna durante la depuración de datos desde estas tablas, o durante el archivado y exportación de datos desde estas tablas.

También se puede actualizar el valor de esta columna durante la importación de datos a un agregador.

Existen tres opciones:

1. De forma predeterminada, el sistema se comporta del mismo modo que en las versiones anteriores: La columna LAST_USED no se tiene en cuenta para depuración, archivado y exportación, no se actualiza durante la importación, y el archivado y la exportación se realizan mediante TIMESTAMP.
2. LAST_USED_FOR_OBJECT_ONLY solo se tiene en cuenta para la tabla GDM_OBJECT.
3. LAST_USED se tiene en cuenta para GDM_CONSTRUCT, GDM_SENTENCE, GDM_OBJECT, GDM_FIELD, GDM_JOIN, GDM_JOIN_OBJECT

Nota: Las opciones 2 y 3 solo se habilitan cuando se ha configurado sniffer para recopilar y actualizar estos datos.
Nota: Validaciones realizadas solo en un recopilador: Si ADMINCONSOLE_PARAMETER.LAST_USED_LOGGING=0, solo se permite TIMESTAMP. Si ADMINCONSOLE_PARAMETER.LAST_USED_LOGGING=1 se permiten todos los parámetros. Si ADMINCONSOLE_PARAMETER.LAST_USED_LOGGING=2, se permiten TIMESTAMP y LAST_USED_FOR_OBJECT_ONLY. En un agregador, se permiten todos los parámetros.

Sintaxis

store aggregator static_data <type>

donde <type> es <TIMESTAMP | LAST_USED | LAST_USED_FOR_OBJECT_ONLY> depende del distintivo last_used logging.

Utilice los mandatos de registro show/store last_used.

Mandato show

show aggregator static_data

store archive_table_by_date

Utilice el mandato de CLI, store archive_table_by_date, solo en agregadores. Utilice este mandato de CLI para archivar todas las tablas estáticas de forma diaria o para archivar datos de tablas estáticas en la primera ejecución y el primer día de cada mes. De forma predeterminada, los datos de archivado de un agregador se ejecutan con tablas estáticas completas diariamente. Si este mandato de CLI se establece en ENABLE, solo se archivarán las tablas estáticas el primer día del mes o la primera vez que se ejecute el archivado de datos.

store run_cleanup_orphans_daily

Utilice este mandato de CLI para limpiar todos los registros antiguos que ya no se utilizan. Este mandato de CLI es relevante para recopiladores y agregadores y, de forma predeterminada, está habilitado.

store run_cleanup_orphans_daily

USO: store run_cleanup_orphans_daily [on|off]

Mandato show

show run_cleanup_orphans_daily

store max_number_collector

Establecer el número máximo de recopiladores que gestiona el agregador. El valor predeterminado es 10.

Mandato show

show max_number_collector

store purge_age_period

Establecer el periodo de antigüedad de la depuración.

Mandato show

show purge_age_period

Tema principal: Visión general de CLI

Mandatos de CLI del alertador

Esta sección lista los mandatos de CLI del alertador.

El subsistema del alertador transmite mensajes que otros componentes han puesto en cola. Por ejemplo, las alertas que el subsistema de detección de anomalías ha puesto en cola o las alertas generadas por las políticas de seguridad. El subsistema del alertador se puede configurar para enviar mensajes a los servidores SMTP y SNMP. Las alertas también se pueden enviar al syslog o las clases de alertas personalizadas, pero no es necesaria ninguna configuración especial para estas dos opciones, solo el arranque del alertador. Existen cuatro tipos de mandatos del alertador. Utilice los enlaces de las listas, o examine los mandatos, que se listan en secuencia alfabética después de las listas.

Mandatos de arranque y sondeo del alertador

- stop alerter
- restart alerter
- store alerter state operational
- store alerter state startup
- store alerter poll
- store anomaly-detection poll
- store anomaly-detection state

Mandatos de configuración de SMTP

- store alerter smtp authentication password
- store alerter smtp authentication type
- store alerter smtp authentication username
- store alerter smtp port
- store alerter smtp relay
- store alerter smtp returnaddr

Mandatos de configuración de SNMP

- store alerter snmp community
- store alerter snmp traphost

restart alerter

Reinicia el alertador. Puede realizar la misma operación utilizando el mandato store alerter state operational, para detener y, a continuación, iniciar el alertador:

store alerter state operational off

store alerter state operational on

Sintaxis

restart alerter

stop alerter

Detiene el alertador.

Puede realizar la misma operación utilizando el mandato store alerter state operational:

store alerter state operational off

Sintaxis

stop alerter

store alerter poll

Inicia (on) o detiene (off) el alertador. El estado predeterminado durante la instalación es off. También puede utilizar los mandatos restart alerter o stop alerter para reiniciar o detener el subsistema del alertador.

Sintaxis

store alerter state operational <on | off>

Mandato show

show alerter state operational

store alerter state operational

Establece el número de segundos, n, que espera el alertador antes de comprobar su cola de mensajes de salida para enviar condiciones de excepción SNMP o transmitir correo electrónico utilizando SMTP. El valor predeterminado es 30.

Sintaxis

store alerter poll <n>

Mandato show

show alerter poll

store alerter state startup

Habilita o inhabilita el inicio automático del alertador durante el arranque del sistema. El estado predeterminado durante la instalación es off.

Sintaxis

store alerter state startup <on | off>

Mandato show

show alerter state startup

store anomaly-detection poll

Establece el intervalo de sondeo de detección de anomalías, en minutos (n). Esto controla la frecuencia con que Guardium comprueba si hay anomalías en los datos del registro.

Sintaxis

store anomaly-detection poll <n>

Mandato show

show anomaly-detection poll

store anomaly-detection state

Habilita o inhabilita el subsistema de detección de anomalías, que ejecuta todas las alertas estadísticas activas, comprueba en los registros si hay anomalías y pone en cola las alertas, según sea necesario para el subsistema de alertador.

Sintaxis

store anomaly-detection state <on | off>

Mandato show

show anomaly-detection state

store alerter smtp authentication password

Establece la contraseña de autenticación SMTP del alertador en el valor especificado. No existe ningún mandato show correspondiente.

Sintaxis

store alerter smtp authentication <value>

store alerter smtp authentication type

Establece el tipo de autenticación requerido por el servidor SMTP en uno de los valores siguientes:

none: Enviar sin autenticación.

auth: Autenticación de nombre de usuario/contraseña. Cuando lo utilice, establezca la cuenta de usuario y la contraseña utilizando los mandatos siguientes:

store alerter smtp authentication username

store alerter smtp authentication password

Sintaxis

store alerter smtp authentication type <none | auth>

Mandato show

show alerter smtp authentication type

store alerter smtp authentication username

Establece el nombre de usuario de autenticación SMTP del alertador en el valor especificado.

Sintaxis

store alerter smtp authentication username <name>

Mandato show

show alerter smtp authentication username

store alerter smtp port

Establece el número de puerto de escucha del servidor SMTP en el valor especificado mediante n. El valor predeterminado es 25 (el puerto estándar de SMTP).

Sintaxis

store alerter smtp port <n>

Mandato show

show alerter smtp port

store alerter smtp relay

Establece la dirección ip del servidor SMTP que debe utilizar el dispositivo Guardium.

Sintaxis

store alerter smtp relay <ip address>

Mandato show

show alerter smtp relay

store alerter smtp returnaddr

Establece la dirección de correo electrónico de devolución para alertas de correo electrónico. Los mensajes rebotados o los errores de correo electrónico se devolverán a esta dirección.

Sintaxis

store alerter smtp returnaddr <email address>

Mandato show

show alerter smtp returnaddr

store alerter snmp community

Establece la comunidad de condiciones de excepción de SNMP que utiliza el alertador en el nombre especificado. No existe ningún mandato show correspondiente.

Sintaxis

store alerter snmp community <name>

store alerter smtp traphost

Establece el servidor de condiciones de excepción SNMP del alertado para que recibirá las alertas, en la dirección IP especificada o el nombre de host DNS.

Sintaxis

store alerter snmp traphost <snmp host>

Mandato show

show alerter snmp traphost

store syslog-trap

Uso: store syslog-trap ON | OFF

Tema principal: Visión general de CLI

Mandatos de CLI de certificados

Utilice los mandatos de certificado para crear una solicitud de firma de certificado (CSR), y para instalar certificados de servidor, CA (entidad emisora de certificados) o certificados de vía de acceso de confianza en el sistema Guardium.

Nota: Guardium no proporciona servicios de entidad emisora de certificados (CA) y no envía sistemas con distintos certificados que el que se ha instalado de forma predeterminada. Un cliente que desea su propio certificado debe ponerse en contacto con una CA de terceros (por ejemplo, VeriSign o Entrust).

Caducidad del certificado

Si caducan los certificados, se pierden funciones. Ejecute el mandato show certificate warn_expire de forma periódica para comprobar certificados caducados. El mandato muestra los certificados que caducarán dentro de seis meses y los certificados que ya han caducado. Ea interfaz de usuario también le informará de los certificados que caducarán. Para ver un resumen de todos los certificados, ejecute el mandato show certificate summary.

Nuevos certificados

Para obtener un certificado nuevo, genere una solicitud firmada de certificado (CSR) y póngase en contacto con una entidad emisora de certificados (CA) como, por ejemplo, VeriSign o Entrust. Guardium no proporciona servicios de CA y no enviará sistemas con certificados diferentes que los que se instalan de forma predeterminada. El formato del certificado debe ser PEM e incluir los delimitadores BEGIN y END. El certificado se puede pegar desde la consola o se puede importar mediante uno de los protocolos de importación estándar.

Nota: No realice esta acción hasta después de que se hayan establecido los parámetros de configuración de red.

create csr

Crea una solicitud firmada de certificado (CSR) para el sistema Guardium. No realice esta acción hasta que se hayan establecido los parámetros de configuración de red. En el CSR generado, se crea automáticamente el nombre común (CN) a partir de los nombres de dominio y host asignados.

create csr alias crea una solicitud de certificado con un alias.

create csr gim crea una solicitud de certificado para gim (Escucha GIM).

create csr gui crea una solicitud de certificado para tomcat.

create csr sniffer crea una solicitud de certificado para sniffer.

Sintaxis

create csr <alias | gimi | gui | sniffer>

restore certificate gim

Restaura el gim de certificados en el último gim de certificados registrado o el gim de certificado predeterminado proporcionado originalmente.

restore certificate gim backup restaura el certificado gim en el último certificado gim de sniffer gim guardado.

restore certificate gim default restaura el certificado gim en el certificado gim predeterminado que se ha suministrado con el sistema.

Sintaxis

restore certificate gim <backup | default>

restore certificate keystore

Restaura el almacén de claves de certificados en el último almacén de claves de certificados o el almacén de claves de certificados predeterminado proporcionado originalmente.

restore certificate keystore backup restaura el almacén de claves de certificados en el último de almacén de claves de certificados guardado.

restore certificate keystore default restaura el almacén de claves de certificados al valor predeterminado proporcionado con el sistema.

Sintaxis

restore certificate keystore <backup | default>

restore certificate mysql

Restaura el certificado de cliente en el último certificado registrado.

restore certificate mysql backup restaura el último certificado mysql guardado.

Sintaxis

restore certificate mysql <backup>

restore certificate mysql backup client

Restaura el certificado de cliente en el último certificado registrado.

restore certificate mysql backup client ca restaura el último certificado guardado de cliente de entidad emisora de certificados (CA).

restore certificate mysql backup client cert restaura el último certificado de cliente guardado.

Sintaxis

restore certificate mysql backup client <ca | cert>

restore certificate mysql backup server

Restaura el certificado de servidor en el último certificado registrado.

restore certificate mysql backup server ca restaura el último certificado guardado de entidad emisora de certificados (CA) de servidor.

restore certificate mysql backup server cert restaura el último certificado de servidor guardado.

Sintaxis

restore certificate mysql backup server <ca | cert>

restore certificate mysql default client

Restaura el certificado de cliente de mysql a la versión predeterminada que se ha suministrado con el sistema.

restore certificate mysql default client ca restaura el certificado de CA de cliente mysql a la versión predeterminada que se ha suministrado con el sistema.

restore certificate mysql default client cert restaura el certificado de cliente mysql a la versión predeterminada que se ha suministrado con el sistema.

Sintaxis

restore certificate mysql default client <ca | cert>

restore certificate mysql default server

Restaura el certificado de servidor de mysql a la versión predeterminada que se ha suministrado con el sistema.

restore certificate mysql default server ca restaura el certificado de CA de servidor mysql a la versión predeterminada que se ha suministrado con el sistema.

restore certificate mysql default server cert restaura el certificado de servidor mysql a la versión predeterminada que se ha suministrado con el sistema.

Sintaxis

restore certificate mysql default server <ca | cert>

restore certificate sniffer

Restaura el certificado en el último certificado registrado.

restore certificate sniffer backup restaura el certificado sniffer en el último certificado sniffer guardado.

restore certificate sniffer default restaura el certificado sniffer en el certificado sniffer predeterminado.

Sintaxis

restore certificate sniffer <backup | default>

restore cert_key mysql backup

Restaura la clave de certificado de cliente o servidor de mysql en el último valor guardado.

restore cert_key mysql backup client restaura la última clave de certificado de cliente mysql guardado.

restore cert_key mysql backup server restaura la última clave de certificado de servidor mysql guardado.

Sintaxis

restore cert_key mysql backup <client | server>

restore cert_key mysql default

Restaura el certificado de cliente de mysql a la versión predeterminada que se ha suministrado con el sistema.

restore cert_key mysql default client restaura la clave de certificado de cliente mysql predeterminada que se ha suministrado con el sistema.

restore cert_key mysql default server restaura la clave de certificado de servidor mysql predeterminada que se ha suministrado con el sistema.

Sintaxis

restore cert_key mysql default <client | server>

show certificate

Muestra el resumen de todos los certificados, la información del certificado, la lista de alias, los certificados del almacén de claves y los certificados caducados o que están a punto de caducar.

Esta autenticación de certificados puede ser verificada mediante una clave pública de Guardium CA (contenida en el certificado de CA que se distribuye con el software de cliente). Este certificado tiene un CN exclusivo de la empresa del cliente (Nombre común, por ejemplo, acme.com, o un CN específico de la máquina (por ejemplo, x4.acme.com). Esto permite que cualquier cliente pueda establecer que el sistema Guardium no solo tiene una certificación válida (es un sistema Guardium real), sino también que es un sistema Guardium específico (o un conjunto de sistemas Guardium) al que se supone que el cliente se debe conectar.

show certificate all visualiza un resumen de todos los certificados.

show certificate alias visualiza una lista de alias.

show certificate gim muestra toda la información de certificado de GIM (Escucha GIM).

show certificate gui muestra toda la información del certificado tomcat.

show certificate keystore muestra todos los certificados del almacén de claves y una lista de alias para que seleccione el certificado que se ha de mostrar.

show certificate mysql muestra la información del certificado de cliente y servidor mysql.

show certificate sniffer muestra toda la información del certificado sniffer.

show certificate stap muestra toda la información de los certificados S-TAP en el almacén de claves.

show certificate summary muestra un resumen de toda la información de certificados.

show certificate trusted muestra toda la información del certificado de confianza.

show certificate warn_expired visualiza todos los certificados caducados o los certificados que caducan dentro de 6 meses.

Sintaxis

show certificate <alias | all | gim | gui | keystore | mysql | sniffer | stap | summary | trusted | warn_expired >

show certificate keystore

Muestra información acerca de los certificados del almacén de claves.

show certificate keystore all muestra todos los certificados del almacén de claves.

show certificate keystore alias muestra una lista de alias para que seleccione el certificado que se ha de mostrar.

Sintaxis

show certificate keystore <all | alias>

show certificate mysql

Muestra la información del certificado mysql.

Parámetros

show certificate mysql client muestra la información del cliente mysql.

show certificate mysql server muestra la información del servidor mysql.

Sintaxis

show certificate mysql <client | server>

store certificate

Almacena un certificado. Pegue el certificado en formato PEM e incluya las líneas BEGIN y END.

Parámetro

store certificate alias almacena un certificado en el almacén de claves después de que se haya generado un CSR. Este mandato de CLI da soporte al mandato de CLI, create csr alias, que permite al usuario crear un certificado de confianza desde cero. Utilice estos dos mandatos para crear certificados de confianza intermedios. Estos certificados de confianza intermedios se pueden utilizar entonces para firmar otros certificados, si es necesario.

store certificate gim permite que el certificado gim personalizado se almacene en el almacén de claves solicitando el certificado, la clave (opcional) y el certificado de CA (Escucha GIM).

store certificate gui almacena el certificado tomcat en el almacén de claves después de que se ha generado un CSR.

store certificate keystore solicita un alias de una palabra para identificar de forma exclusiva el certificado de confianza y almacenarlo en el almacén de claves.

store certificate mysql almacena los certificados de cliente y servidor.

store certificate sniffer almacena certificados de sniffer.

store certificate stap almacena certificados de S-TAP.

Sintaxis

store certificate <gim | gui | keystore | mysql | sniffer | stap >

store certificate mysql client

Almacena un certificado de cliente mysql.

store certificate mysql client ca almacena certificados de entidad emisora de certificados (CA) de cliente.

store certificate mysql client cert almacena los certificados de cliente.

Sintaxis

store certificate mysql client <ca | cert>

store certificate mysql server

Almacena un certificado de servidor mysql.

store certificate mysql server ca almacena certificados de entidad emisora de certificados (CA) de servidor.

store certificate mysql server cert almacena certificados de servidor.

Sintaxis

store certificate mysql server <ca | cert>

store cert_key

Almacena la clave de certificado del sistema y la clave de certificado de un servidor y cliente de mysql.

store cert_key mysql almacena la clave de certificado de un servidor y cliente de mysql.

store cert_key sniffer almacena la clave de certificado de sniffer.

Sintaxis

store cert_key <mysql | sniffer>

store cert_key mysql

Almacena la clave de certificado de un servidor o cliente de mysql.

store cert_key myself client almacena la clave de certificado de un cliente de mysql.

store cert_key myself server almacena la clave de certificado de un servidor de mysql.

Sintaxis

store cert_key mysql <client | server>

store cert_key sniffer

Almacena la clave de certificado del sistema. Este mandato permite al usuario establecer el certificado del sistema utilizado por el sistema Guardium (en comunicación con S-TAP). El certificado se puede pegar desde la consola o se puede importar mediante uno de los protocolos de importación estándar. El formato del certificado debe ser PEM y debe incluir los delimitadores BEGIN y END. Este certificado tiene que estar firmado por una CA cuyo certificado autofirmado esté disponible para el software S-TAP mediante guardium_ca_path.

store cert_key sniffer console almacena la clave de certificado de sniffer pegando la clave en la consola.

store cert_key sniffer import almacena la clave de certificado de sniffer importando el archivo de certificados.

Sintaxis

store cert_key sniffer <console | import>

Opciones backup o default

Puede optar por restaurar los certificados y las claves de certificados con el parámetro backup o default. Utilice el parámetro backup para restaurar un certificado en el último certificado guardado. Utilice el parámetro default para restaurar un certificado en el certificado original proporcionado por Guardium.

Fechas de caducidad de certificados y mandatos de resumen

Ejecute el mandato show certificate warn_expire de forma periódica. Este mandato le avisa de los certificados que caducarán en seis meses y muestra una lista de los certificados caducados. Para obtener más información, consulte el mandato show certificate CLI. Para ver un resumen de todos los certificados, ejecute el mandato de CLI show certificate summary. Ejecute los mandatos periódicamente para revisar las fechas de caducidad de los certificados.

Tema principal: Visión general de CLI

Mandatos de CLI de configuración y control

Utilice los siguientes mandatos de CLI para configuración y control.

? (signo de interrogación)

Cuando escriba un mandato, escriba un signo de interrogación en cualquier punto para visualizar los argumentos.

Sintaxis

<partial_command> ?

Ejemplo

CLI> show account strike ?

USO: show account strike <arg>, donde arg es:

?, count, interval, max

ok

CLI>

delete unit type

Utilice este mandato para borrar uno o varios atributos de tipo de unidad. Tenga en cuenta que con este mandato no se pueden borrar todos los atributos de tipo de unidad. Para obtener más información, consulte la tabla que se encuentra después del mandato store unit type.

Sintaxis

delete unit type [manager | standalone] [aggregated] [netinsp] [network routes static] [stap] [mainframe]

commands

Muestra una lista alfabética de todos los mandatos de CLI.

Sintaxis

commands

debug

Habilitar/inhabilitar la modalidad de depuración. Sin un argumento, conmuta el estado de depuración. Opcionalmente, se puede pasar un argumento de estado.

Sintaxis

debug <on | off>

eject

Este mandato desmonta y expulsa el CD ROM, lo que resulta útil después de actualizar o volver a instalar el sistema o de instalar parches distribuidos mediante un CD ROM.

Sintaxis

eject

delete scheduled-patch

Para suprimir una solicitud de instalación de parche, utilice el mandato de CLI delete scheduled-patch

Consulte el mandato de CLI, store system patch install para obtener más información sobre la instalación del parche.

forward support email

Cuando está habilitada la opción support-state (el valor predeterminado), este mandato establece la dirección de correo electrónico que recibirá las alertas del sistema.

Sintaxis

forward support email to <dirección de correo electrónico>

Mandato show

show support-email

iptraf

IPTraf es un programa de utilidad de estadísticas de red que se distribuye con el sistema operativo subyacente. Recopila información diferente, tal como un paquete de conexión TCP y los recuentos de bytes, las estadísticas de la interfaz y los indicadores de actividad, los desgloses de tráfico TCP/UDP, el paquete de estación LAN y los recuentos de bytes. El manual de usuario de IPTraf se puede encontrar en la ubicación siguiente, (si este enlace no funciona, es posible que esté disponible en otras ubicaciones):

http://iptraf.seul.org/2.7/manual.html

Sintaxis

iptraf

license check

Indica si la licencia instalada es válida. Utilice este mandato después de instalar una nueva clave de producto.

Sintaxis

license check

ping

Envía paquetes de ping ICMP a un host remoto. Este mandato resulta útil para comprobar la conexión de red. El valor de host puede ser una dirección IP o nombre de host.

Sintaxis

ping <host>

quit

Sale de la interfaz de línea de mandatos.

Sintaxis

quit

recover failed

Este mandato restaura los archivos de transferencia CSV/CEF/PDF y los vuelve a colocar en la carpeta de exportación para que se pueda volver a intentar la exportación.

Sintaxis

recover failed [csv|cef|pdf]

register management

Registra el sistema Guardium para que lo gestione el Gestor central especificado. Se guarda la configuración de registro previo de este sistema Guardium y, si la unidad no está registrada, esta configuración se restaurará posteriormente.

Sintaxis

register management <ip gestor> <puerto>

Parámetros

ip gestor es la dirección IP del gestor central.

puerto es el número de puerto que utiliza el gestor central (normalmente 8443).

restart gui

Reinicia la interfaz web de IBM® Guardium. Para planificar opcionalmente un reinicio de la GUI una vez al día o una vez a la semana, utilice parámetros adicionales. HH indica las horas 01-24. MM indica los minutos 01-60. W es el día de la semana 0-6, para domingo es 0. Si figura dos veces HHMM, solo se utiliza la última entrada. El parámetro clear suprime la hora planificada.

Para reiniciar los procesos del clasificador y los asesoramientos de seguridad, ejecute el mandato restart gui en la CLI (no desde la GUI).

Si se ejecuta restart GUI en la GUI, solo se reinician los servicios web. Es necesario ejecutar el mandato restart GUI desde la CLI para reiniciar por completo todos los procesos, incluidos los procesos del clasificador y de los asesoramientos de seguridad. Es necesario ejecutar el mandato restart GUI desde la CLI para que cada unidad gestionada reinicie el escucha del clasificador.

Sintaxis

restart gui [HHMM|HHMMW|clear]

restart stopped_services

Utilice este mandato de CLI para reiniciar los servicios que se han detenido previamente con el mandato store auto_stop_services_when_full.

Sintaxis

restart stopped_services

restart system

Reinicia el sistema Guardium. El sistema realiza una conclusión completa y se reinicia, lo que significa que finalizará la sesión de CLI.

Sintaxis

restart system

show buffer

Este mandato muestra un informe del uso del almacenamiento intermedio para el proceso del motor de inspección. Si tiene problemas de carga, es posible que el servicio de soporte técnico de IBM le solicite que ejecute este mandato.

Sintaxis

show buffer <log | snif>

show buffer log

Utilice este mandato de CLI para visualizar el uso del almacenamiento intermedio por parte del proceso del motor de inspección.

show buffer snif

Utilice este mandato de CLI para visualizar el uso del almacenamiento intermedio por parte de Sniffer.

show build

Muestra información del build del software instalado (build, release, versión de snif).

Sintaxis

show build

show defrag

Identifica los paquetes fragmentados e intenta volver a crear los paquetes antes de que lleguen al proceso de sniffing de red. La desfragmentación solo es relevante para sniffing de red a través de un dispositivo TAP o SPAM.

Sintaxis

show defrag

Parámetros

Packet size: El tamaño del paquete en bytes, con un máximo de 217 (131072)

Time interval: El intervalo de tiempo

Trigger level: El nivel de desencadenante

Release level: El nivel de release especificado como un número de segundos, con un máximo de 31 a la potencia de dos (2147483648).

show network routes static

Permitir que el usuario solo tenga una dirección IP por dispositivo (mediante eth0) y direccionar el tráfico a través de diferentes direccionadores mediante tablas de direccionamiento estático. Lista los direccionamientos estáticos actuales con sus ID.

Sintaxis

show network routes static

Mandato delete

delete network routes static

show password

Este mandato de CLI muestra las funciones de contraseña. Con password disable [0|1] se elimina el uso de una contraseña almacenando el valor 1. Con password expiration [CLI|GUI] [Número de días] se muestra el número de días entre los cambios de contraseña obligatorios. El valor predeterminado es de 90 días. Password Validation [ON|OFF] determina si la contraseña es fuerte.

Sintaxis

show password disable [0|1]

show password expiration [CLI|GUI] 90

show password validation [ON|OFF]

show security policies

Muestra la lista de políticas de seguridad.

Sintaxis

show security policies

show system patch available

Muestra los parches instalados y los parches planificados para ser instalados, junto con la fecha/hora y el estado de la instalación.

Sintaxis

show system patch installed

show system patch installed

Muestra los parches instalados y los parches planificados para ser instalados, junto con la fecha/hora y el estado de la instalación.

Sintaxis

show system patch installed

show system public key

Muestra la clave pública para cli o tomcat. Si no existe ninguna, el mandato crea una.

Nota: Consulte show system key, store system key en la sección de Mandatos de CLI de certificados.

Sintaxis

show system public key <cli | tomcat | grdapi>

stop gui

Detiene la interfaz de usuario web.

Sintaxis

stop gui

stop system

Detiene y apaga el dispositivo.

Sintaxis

stop system

store apply_user_hierarchy

Utilice este mandato de CLI para aplicar la jerarquía de usuarios al receptor de la auditoría.

Si el valor es ON, el receptor del grupo no de auditoría, esto es, el receptor que no es el receptor del grupo de auditoria (normal o rol), solo verá los resultados con una IP de grupo situada por debajo de la jerarquía del receptor, incluido el receptor.

Sintaxis

store apply_user_hierarchy [ON | OFF]

Mandato show

show apply_user_hierarchy

store allow_simulation

Habilita (on) o inhabilita (off) la función para ejecutar la simulación de políticas en el dispositivo.

Para ejecutar la simulación, se debe reproducir el tráfico original mediante el motor de reglas (con la política que se necesita probar). Este requiere guardar una parte del SQL con sus valores en el dispositivo. Si se habilita o inhabilita allow_simulation, se indica a IBM Guardium que guarde o NO guarde cualquier SQL o valor.

Sintaxis

store allow_simulation [on|off]

Mandato show

show allow_simulation

store alp_throttle

Utilice este mandato de CLI para regular la cantidad de datos que se han de registrar.

Uso: store alp_throttle <núm>

donde <núm> es el número, en un rango de -2147483647 y 2147483647.

El valor predeterminado es 0.

0 - no registrar en GDM_FLAT_LOG y no crear archivos tapks

>0 - registrar en GDM_FLAT_LOG y no crear archivos tapks

<0 - registrar en GDM_FLAT_LOG y crear archivos tapks

99999 - no registrar en GDM_FLAT_LOG pero crear archivos tapks.

Ejemplo

10 - registrar en GDM_FLAT_LOG 10% de sentencias.

10 - registrar en GDM_FLAT_LOG 10% de sentencias y crear archivos tapks

store analyzer

Omitir sesión: Se omiten la solicitud actual y el resto de la sesión. Esta acción registra una infracción de política pero detiene el registro de construcciones y no prueba las infracciones de política de ningún tipo durante el resto de la sesión. Esta acción puede ser útil si, por ejemplo, la base de datos incluye una región de prueba y no es necesario aplicar reglas de política en dicha región de la base de datos.

Este mandato establece el valor del periodo de espacio de la sesión que se ha de omitir y la duración de dicha sesión.

Sintaxis

store analyzer [ignore_sess_timeout | max_open_sess]

Mandato show

show analyzer

store auto_stop_services_when_full

Si el valor es ON, se detienen los servicios internos cuando la base de datos está llena por encima del umbral del 90%.

Se detienen el motor de inspección, la clasificación y otros servicios relacionados con la recopilación. Asimismo, la importación o restauración de agregaciones no procesar ningún archivo nuevo.

Para solucionarlo, utilice los diferentes mandatos support (support clean audit_task, support clean log_files, support clean DAM_data, support show large_files) para analizar y depurar manualmente las tablas de gran tamaño.

Sintaxis

store auto_stop_services_when_full [ON | OFF]

Mandato show

show auto_stop_services_when_full

store connect oracle_parser

Utilice este mandato para conectar y desconectar el analizador Oracle del analizador DB2. El valor predeterminado es OFF (desconectar).

Sintaxis

store connect oracle_parser [ON | OFF]

Uso: store connect_oracle_parser [estado], donde estado es ON/OFF. ON es para conectar y OFF es para desconectar.

Mandato show

show connect oracle_parser

store csv_fetch_size

CSV_FETCH_SIZE y CSV_MAX_SIZE son parámetros GLOBAL_PROFILE que solo se pueden modificar mediante CLI.

Se pueden descargar los informes de Guardium en formato de archivo CSV.

CSV_MAX_SIZE se utiliza para controlar el tamaño de la descarga de CSV que se recupera cuando se pulsa Descargar todos los registros en el menú de exportación de informes.

CSV_FETCH_SIZE lo utiliza el servicio REST de informes para controlar el número total de registros.

Nota: csv_max_size requiere un reinicio de la GUI para que los cambios entren en vigor. csv_fetch_size no requiere un reinicio de la GUI para que los cambios entren en vigor.

Mandato show

CLI> show csv_fetch_size

Uso

CLI> store csv_fetch_size

USO: store csv_fetch_size <número>

donde el número es mayor que 0

store csv_max_size

CSV_FETCH_SIZE y CSV_MAX_SIZE son parámetros GLOBAL_PROFILE que solo se pueden modificar mediante CLI.

Se pueden descargar los informes de Guardium en formato de archivo CSV.

CSV_MAX_SIZE se utiliza para controlar el tamaño de la descarga de CSV que se recupera cuando se pulsa Descargar todos los registros en el menú de exportación de informes.

CSV_FETCH_SIZE lo utiliza el servicio REST de informes para controlar el número total de registros.

Nota: csv_max_size requiere un reinicio de la GUI para que los cambios entren en vigor. csv_fetch_size no requiere un reinicio de la GUI para que los cambios entren en vigor.

Mandato show

CLI> show csv_max_size

Uso

CLI> store csv_max_size

USO: store csv_max_size <número>

donde el número es mayor que 0

store default_queue_size

Utilice este mandato de CLI para controlar el parámetro de configuración ADMINCONSOLE_PARAMETER.DEFAULT_QUEUE_SIZE. El valor predeterminado es 25. El rango es 25-300.

Se debe reiniciar sniffer después de cambiar el valor.

Sintaxis

store default_queue_size <N>, donde N es el número en un rango de 25 a 300

Mandato show

show default_queue_size 25

store defrag

Utilice este mandato para restaurar los valores predeterminados de desfragmentación o para establecer el tamaño de la desfragmentación. Después de especificar este mandato, debe emitir el mandato restart inspection-core para que los cambios entren en vigor. La desfragmentación solo es relevante para sniffing de red a través de un dispositivo TAP o SPAM.

Sintaxis

store defrag [default | size <s> interval <i> trigger <t> release <r>]

Mandato show

show defrag

Parámetros

default: Restaurar el tamaño predeterminado.

s: El tamaño del paquete en bytes, con un máximo de 217 (131072)

i: El intervalo de tiempo

t: El nivel de desencadenante

r: El nivel de release especificado como un número de segundos, con un máximo de 31 a la potencia de dos (2147483648).

store delayed_firewall_correlation

Utilice este mandato de CLI para retener una conexión de usuario hasta que se haya llevado a cabo la correlación de descifrado.

Sintaxis

store delayed_firewall_collection [on | off]

Mandato show

show delayed_firewall_correlation

store full-bypass

Este mandato se ha diseñado solo para casos de emergencia, cuando el sistema Guardium bloquea el tráfico de forma imprevista. Si el valor es on, todo el tráfico de red pasa directamente a través del sistema y el sistema Guardium no lo ve.

Cuando se utilice este mandato, se le solicitará la contraseña del usuario administrador.

Sintaxis

store full-bypass <on | off>

store gdm_analyzer_rule

Reglas del analizador: Determinadas reglas se pueden aplicar en el nivel del analizador. Los ejemplos de reglas del analizador son: conjuntos de caracteres definidos por el usuario, cambios del programa de origen y las modalidades de vigilancia de cortafuegos o no vigilancia de cortafuegos. En los releases anteriores, las políticas y reglas se aplicaban al final del proceso de la solicitud en el estado de registro. En algunos casos, esto comportaba un retraso en la toma de decisiones basadas en estas reglas. Si las reglas se aplican en el nivel del analizador, se pueden tomar decisiones en una fase más temprana.

Nota: Cuando se aplican las reglas del analizador en los cambios del programa de origen, si el programa de origen no coincide con el patrón exacto, añada .* al final del patrón por si el programa de origen incluye un espacio de cola (que el usuario no ha visto).

Sintaxis

store gdm_analyzer_rule [active_flag | new]

store gdm_analyzer_rule active_flag

Uso: store gdm_analyzer_rule active_flag <id> <on|off>

donde <id> es el ID de regla.

Utilice el mandato de CLI, show gdm_analyzer_rule, para ver una lista de las reglas del analizador GDM.

store gdm_analyzer_rule new

Escriba una descripción de la regla (opcional):

Escriba un tipo de regla (opcional):

Mandato show

show gdm_analyzer_rule

store gdm_analyzer_rule new

Utilice el mandato de CLI de Guardium para añadir una regla de analizador para añadir una expresión regular directa al patrón de la serie de UID de máscara.

CLI> store gdm_analyzer_rule new

Please enter rule description: new rule 4

Tipo de regla:

1. Cambiar programa de origen

2. Establecer juego de caracteres alternativo

3. Enviar veredicto

4. Excluir HADOOP

5. Definir protocolo y puerto

6. Omitir sesión después de paquetes

7. Establecer usuario de BD Oracle vacío si falta información de inicio de sesión

8. Forzar inicio de sesión de MS SQL

9. Transformar serie

Please select rule type (required): 9

Please enter pattern (required, regex string): (.*)(-ppassword)(.*)

Please enter format (required, regex string): \\\\1-p****\\\\3

Do you want to activate the rule now? (Yes/No)

Y

ok

store gdm_http_session_template

Utilice este mandato de CLI para establecer la plantilla para la sesión HTTP.

Uso

```
store gdm_http_session_template [activate] [add] [deactivate] [remove]
```

Mandato show

```
show gdm_http_session_template
```

Attempting to retrieve the template information. It may take time. Please wait.

Tabla 1. store gdm_http_session_template

ID#	Regex URL activo	Session Regex	Username Regex	Login_Session Regex	Comentario	Logout_Session_ID	Logout_URL_Regex
1	1	Cookie.*PHPSESSID=([[:a	.*user_name=([[:alnum:]	Set-Cookie:.*PHPSESSID=	ejemplo de sesión HTTP suprimida		
2	1	Cookie.*PSJSESSIONID=([	.*SignOnDefault=([[:aln		ejemplo de sesión HTTP	cmd=logout	
3	1	Cookie.*JSESSIONID=([0-	.*username=([[:alnum:]]	Set-Cookie:.*JSESSIONID	ejemplo de sesión HTTP		Logout.jsp

store log external

Utilice este mandato para establecer el tamaño de archivo, el periodo de vaciado, el error gdm y el estado del registro externo.

Esta regla SOLO se muestra si se ejecuta el mandato de CLI siguiente:

store log external state on

A continuación, el registro externo se muestra como una acción de política

Mandato de CLI para comprobar el estado:

show log external state

Mandato de CLI para habilitar o inhabilitar esta acción:

store log external state on/off

Uso

```
store log external [file_size] [flush_period] [gdm_error] [state]
```

Uso: store log external gdm_error <state>

donde state es on/off. 'on' es para habilitar y 'off' para inhabilitar.

Uso: store log external file_size <num>

donde <num> es el tamaño de archivo.

El valor predeterminado es de 4096 días.

Uso: store log external flush_period <num>

donde <num> es el periodo de vaciado.

El valor predeterminado es de 60 segundos.

Uso: store log external state <state>

donde state es on/off. 'on' es para habilitar y 'off' para inhabilitar.

Mandato show

```
show log external [file_size] [flush_period] [gdm_error] [state]
```

store monitor gdm_statistics

Utilice este mandato de CLI para obtener información acerca de la utilización de la unidad. El valor predeterminado es 1 (ejecutar el script cada hora).

Sintaxis

```
CLI> store monitor gdm_statistics
USO: store monitor gdm_statistics <hora>, donde hora es un valor de 0 a 24.
       El valor predeterminado es 1, lo que significa ejecutar el script cada hora.       El valor 0, significa no ejecutar el
script.
```

Mandato show

CLI> show monitor gdm_statistics

Disable gdm_statistics monitor

store gui

store gui [port | session_timeout | csrf_status]

Establece el número de puerto TCP/IP en que la interfaz de gestión de dispositivos IBM Guardium acepta conexiones. El valor predeterminado es 8443. **n** debe ser un valor con un rango de 1024 a 65535. Asegúrese de que evita utilizar cualquier puerto que sea necesario o que se utilice con otro fin.

Establece session_timeout: Define el periodo de tiempo (en segundos) sin actividad antes de que se supere el tiempo de espera. Cuando se supera el tiempo de espera sin actividad, se debe volver a iniciar sesión en IBM Guardium. El periodo predeterminado es de 900 segundos (15 minutos).

Establece CSRF (Cross-site Report Forgery) (ON | OFF): Consulte la sección **Errores de permisos CSRF y 403** en el tema de ayuda Iniciación a la GUI. De forma predeterminada está habilitado en un sistema actualizado. Si intenta utilizar algunas funciones del navegador web (por ejemplo, F5/Ctrl-R/Renovar/Volver a cargar, Retroceder/Avanzar) se genera un mensaje de error de permiso 403.

El nuevo valor de tiempo de espera de sesión entra en efecto después del siguiente reinicio de la GUI.

Sintaxis

store gui port <n>

store gui session_timeout <n>

store gui csrf_status [on | off]

Mandato show

Muestra el número de puerto, el estado, el tiempo de espera de sesión (en segundos) y el estado CSRF de la GUI.

Sintaxis

show gui [port | state | all | session_timeout | csrf_status]

store gui cache

Utilice este mandato de CLI para habilitar o inhabilitar (ON/OFF) el almacenamiento en caché del navegador web.

La respuesta es

The parameter has been changed.

Restarting gui

Changing to port 8443

Stopping.....

Safekeeping xregs

ok

De forma predeterminada, el almacenamiento en caché está habilitado.

Si se cambia el valor de caché, automáticamente se reinicia el servidor web de Guardium.

En Firefox, para que el valor entre en vigor, se tiene que borrar la caché en los navegadores respectivos.

Sintaxis

store gui cache [ON | OFF]

Mandato show

show gui cache

store gui session_timeout

Establece el periodo de tiempo (en segundos) sin actividad antes de que se supere el tiempo de espera. Cuando se supera el periodo tiempo de espera sin actividad, se debe volver a iniciar sesión en IBM Guardium. El periodo predeterminado es de 900 segundos (15 minutos).

Sintaxis

store gui session_timeout

Mandato show

show gui session_timeout

store gui csrf_status

Utilice este mandato de CLI para habilitar o inhabilitar el estado de CSRF (Cross-site Request Forgery).

Sintaxis

store gui scrf_status [on | off]

Mandato show

show gui scrf_status

store gui xss_status

Utilice este mandato de CLI para habilitar o inhabilitar el estado de XSS (Cross-Site Scripting). De forma predeterminada, esta opción está habilitada en sistemas actualizados.

Sintaxis

store gui xss_status [on | off]

Mandato show

show gui xss_status

store gui hsts_status

Utilice este mandato de CLI para habilitar o inhabilitar el estado de HSTS (HTTP Strict Transport Security Filter). De forma predeterminada, esta opción está inhabilitada en sistemas actualizados y se recomienda activarla después de instalar los certificados válidos. Para obtener más información, consulte el tema: Cómo instalar un certificado para evitar un desafío de certificados SSL de navegador.

Sintaxis

store gui hsts_status [on | off]

Mandato show

show gui hsts_status

store installed security policy

Establece la política de seguridad con el nombre **policy-name** como la política de seguridad instalada.

Sintaxis

store installed security policy <policy-name>

Mandato show

show installed security policy

store keep_psmls

Utilice este mandato de CLI para retener los diseños/perfiles/portlets actuales que han creado los usuarios de la aplicación Guardium. Establezca este mandato de CLI en ON antes de una actualización y se retendrá el valor de psmls de la versión actual.

Sintaxis

store keep_psmls [ON | OFF]

show keep_psmls

store ldap-mapping

Parámetros de Almacenar correlación de LDAP - permite una correlación personalizada del esquema del servidor LDAP. Este mandato permite realizar una correlación personalizada del esquema del servidor LDAP con los atributos de correo electrónico, nombre y apellidos (email, firstname y lastname). Se utiliza el parámetro paging para facilitar la transferencia entre cualquier tipo de servidor LDAP (Active Directory, Novell Directory, Open LDAP, Sun One Directory, Tivoli Directory). Si el parámetro paging se establece en on, pero el servidor no admite la paginación, se realiza la búsqueda sin paginación.

Ejemplo para paging. Si el mandato de CLI **ldap-mapping paging** se establece en ON, Microsoft Active Directory descarga el número máximo de usuarios definidos con el valor de límite en la pantalla Configuración de la importación LDAP. Si el mandato de CLI **ldap-mapping paging** se establece en OFF, Active Directory solo descarga un máximo de 1000 usuarios, independientemente del valor de límite establecido. Todas las otras configuraciones de servidor LDAP deben utilizar el mandato de CLI **ldap-mapping paging off** para poder descargar usuarios hasta el valor establecido como límite.

Nota: Cada vez que cambia los atributos del mandato de CLI ldap-mapping, antes de la actualización también debe seleccionar Reemplazar cambios existentes en la pantalla de configuración de la importación de LDAP en la GUI de IBM Guardium. Esta acción se debe llevar a cabo cada vez que cambia los atributos email, firstname o lastname del mandato de CLI ldap-mapping e importa usuarios LDAP.

Mandatos show

show ldap-mapping [email] [firstname][lastname] <name>

show ldap-mapping paging ON|OFF

Es necesario reiniciar la GUI donde se ejecuta CLI para que entren en vigor los nuevos parámetros.

Ejemplos

Estos son algunos ejemplos.

store ldap-mapping firstname name

store ldap-mapping lastname sn

store ldap-mapping email mail

store ldap-mapping paging on

Si se escriben los atributos de este modo, el proceso de correlación utiliza el primer atributo que encuentra. Si esto no es lo que desea, utilice uno de los ejemplos para correlacionar atributos específicos.

Valores para el atributo firstname: gn,givenName,name

Valores para el atributo lastname: sn,surname,name

Valores para el atributo email: userPrincipalName,mail,email,emailAddress,pkcs9email,rfc822Mailbox

Valores para paging: on, off

store license

Este mandato aplica una nueva clave de licencia al dispositivo.

Una clave de licencia puede ser de dos tipos: Sustitución y adición. Una clave de sustitución sustituye la licencia instalada actualmente, mientras que una clave de adición se añade a la licencia actual instalada. Las licencias de tipo adición solo pueden añadir funciones. Las nuevas funciones se pueden habilitar y, cuando sea necesario, se pueden actualizar las fechas de caducidad, se aumentará el número de exploraciones y orígenes de datos y se sustituirán determinados campos numéricos de la licencia, tales como el número de unidades gestionadas.

Sintaxis

store license

Mandato show

show license

Ejemplo

Cuando utilice el mandato store license, se le solicitará que pegue la nueva clave de producto:

CLI> store license

Pegue la serie enviada por IBM Guardium y, a continuación, pulse Intro.

Copie y pegue la nueva clave de producto en la ubicación del cursor y, a continuación, pulse Intro. La clave del producto no contiene saltos de línea ni caracteres de espacio en blanco y siempre termina con (e incluye) un signo igual de cola. Se muestra una serie de mensajes que terminan con:

Le recomendamos que reinicie la máquina lo antes que pueda para poder completar el proceso de actualización de la licencia.

ok

CLI>

Ejecute el mandato restart gui en este momento.

store log classifier level

Establece el nivel de depuración para el clasificador en uno de los valores que se muestran.

Sintaxis

store log classifier level DEBUG|INFO|WARN|ERROR|FATAL

Mandato show

show log classifier level

store log sql parser_errors

Establece el registro de los mandatos SQL con errores de sintaxis.

Sintaxis

store log sql parser_errors [on|off]

Nota: Es necesario reiniciar el motor de inspección después de emitir el mandato store para aplicar el cambio.

Mandato show

show log sql parser_errors

store log object_join_info

Establece el registro de object_join.

Una tabla de unión es un modo de implementar relaciones de muchos a muchos. Utilice la entidad join para unir tablas en una sentencia SQL SELECT.

Sintaxis

store log object_join_info [on | off]

Mandato show

show log object_join_info

store log session_info

Relacionado con Sniffer

Sintaxis

store log session_info [on | off]

Mandato show

show log session_info

store log exception sql

Cuando su valor es **on**, registra el mandato SQL completo durante el registro de excepciones.

Sintaxis

store log exception sql <on | off>

Mandato show

show log exception sql

store logging granularity

Establece la granularidad del registro en el número de minutos especificado. Debe utilizar uno de los valores de minutos que se muestran en la sintaxis. El valor predeterminado es 60.

Sintaxis

store logging granularity <1, 2, 5, 10, 15, 30 o 60>

Mandato show

show logging granularity

store max_audit_reporting

Muestra el umbral del informe de auditoría. El valor predeterminado es 32. Cuando define informes en el proceso de auditoría el número de días del informe, que se define con los campos FROM-TO, no debe superar un umbral determinado, cuyo valor predeterminado es un mes. Consulte la sección Proceso de flujo de trabajo, gestión central y agregación del tema de ayuda Automatización del flujo de trabajo de cumplimiento, para obtener más información acerca de cómo utilizar este mandato de CLI.

Sintaxis

store max_audit_reporting

Mandato show

show max_audit_reporting

store max_result_set_size

El valor predeterminado de store max_result_set_size es 100 (el tamaño es entre 1 y 65535) y ayuda a ajustar el motor de inspección cuando se observan los datos devueltos. Este mandato establece el límite del tamaño total del conjunto de resultados. Este parámetro funciona para cualquier tipo de base de datos. Si el valor supera el umbral definido, el analizador no recibe los datos para calcular el valor de registros afectados.

Sintaxis

store max_result_set_size <size>

Mandato show

show max_result_set_size

store max_result_set_packet_size

El valor predeterminado de store max_result_set_packet_size es 32 (el tamaño es entre 1 y 65535) y ayuda a ajustar el motor de inspección cuando se observan los datos devueltos. Este mandato establece el límite del tamaño de paquete en la respuesta. Este parámetro funciona para cualquier tipo de base de datos. Si el valor supera el umbral definido, el analizador no recibe los datos para calcular el valor de registros afectados.

Sintaxis

store max_result_set_packet_size <size>

Mandato show

show max_result_set_packet_size

store max_tds_response_packets

El valor predeterminado de store max_tds_response_packets es 5 (el tamaño es entre 1 y 65535) y ayuda a ajustar el motor de inspección cuando se observan los datos devueltos. Este mandato establece el límite del número de paquetes de la respuesta. Este parámetro solo funciona para MS SQL. Si el valor supera el umbral definido, el analizador no recibe los datos para calcular el valor de registros afectados.

Sintaxis

store max_tds_response_packets <size>

Nota: max_tds_response_packets (Corriente de datos tabulares) solo es aplicable para MS SQL Server y Sybase.

Mandato show

show max_tds_response_packets

store maximum query duration

Establece el número máximo de segundos para una consulta en el valor especificado en **n**. El valor predeterminado es 180. Se le recomienda que **no** lo establezca en un valor mayor al valor predeterminado porque aumenta la posibilidad de una sobrecarga del sistema durante el proceso de la consulta. Este valor también se puede establecer desde el panel Ejecutar supervisor de estado del portal del administrador.

Sintaxis

store maximum query duration <n>

Mandato show

show maximum query duration

store monitor [buffer | custom_db_usage | gdm_statistics]

Utilice el mandato de CLI store monitor buffer para establecer el intervalo de la frecuencia en que debe ejecutarse el script que recupera la información que se muestra en el informe Supervisor de uso de almacenamiento intermedio del separador Supervisor de IBM Guardium.

Sintaxis: store monitor buffer

Utilice el mandato de CLI store monitor custom_db_usage para establecer el estado en on y para especificar la hora de ejecución de este trabajo.

Sintaxis

```
CLI> store monitor custom_db_usage
USO: store monitor custom_db_usage <state> <hour>
donde state es on/off.
Si el valor de state es on, especifique la hora de ejecución.
El valor válido es un número de 0 a 23
```

Utilice este mandato de CLI store monitor gdm_statistics para obtener información acerca de la utilización de la unidad. El valor predeterminado es 1 (ejecutar el script cada hora).

Sintaxis

```
CLI> store monitor gdm_statistics
USO: store monitor gdm_statistics <hora>, donde hora es un valor de 0 a 24.
       El valor predeterminado es 1, lo que significa ejecutar el script cada hora.       El valor 0, significa no ejecutar el
script.
```

Mandatos show

show monitor buffer

show monitor custom_db_usage

show monitor gdm_statistics

store mysql_utf8mb4

Habilitar el soporte para la codificación UTF-8 de 4 bytes (utf8mb4).

Este mandato modifica los procesos Sniffer de Guardium y las bases de datos internas para capturar y almacenar correctamente los caracteres UTF-8 de 4 bytes. Habilitar utf8mb4 puede resultar útil si los orígenes de datos de su entorno contienen caracteres de 4 bytes como los que se utilizan, por ejemplo, en ideogramas chinos,

japoneses y coreanos.

Tenga en cuenta lo siguiente cuando utilice este mandato:

- El proceso adicional necesario para capturar y almacenar los caracteres de 4 bytes afecta de forma negativa al rendimiento de su sistema Guardium. Por este motivo, no habilite utf8mb4 a menos que requiera soporte de caracteres de 4 bytes en su entorno.
- Si se requiere el soporte de la codificación UTF-8 de 4 bytes en un entorno gestionado centralmente o agregado, se debe habilitar utf8mb4 en todos los sistemas Guardium del entorno. Si solo se habilita utf8mb4 en algunos sistemas del entorno pueden surgir problemas, tales como, errores de agregación o una visualización incorrecta de los informes.
- Los datos recopilados o agregados antes de habilitar utf8mb4 continúan estando disponibles y funcionan correctamente después de habilitar utf8mb4.

PRECAUCIÓN:
Después de habilitar el soporte de UTF-8 de 4 bytes con el mandato store mysql_utf8mb4, el cambio no se puede deshacer ni revertir. Después de habilitar utf8mb en un sistema Guardium, el único modo de eliminar el soporte de caracteres UTF-8 de 4 bytes es volver a crear por completo el sistema.

Sintaxis

store mysql_utf8mb4

Mandato show

show mysql_utf8mb4

Ejemplo

```
> show mysql_utf8mb4
mysql configuration NOT set with UTF8MB4.
ok

> store mysql_utf8mb4
Attempting to change the mysql config file. It may take time. Please wait.
Start to modify mysql config file
Restarting mysql
Mysql has been restarted. Please exit CLI and log back on.
The parameter IS_UTF8MB4 has been changed to 1.

> show mysql_utf8mb4
mysql configuration set with UTF8MB4.
ok
```

store packet max-size

Limitar el tamaño máximo de paquetes de Sniffer.

Sintaxis

store packet max-size 1536

Mandato show

show packet max-size

store pdf-config

Utilice este mandato para cambiar el tamaño de font de pdf y la orientación de pdf del contenido del cuerpo de la imagen PDF (excepto la cabecera y el pie de página).

La unidad de tamaño está en el rango de 1 (más pequeña) a 10 (más grande) y el valor predeterminado es 6.

La unidad de orientación es 1 (para la orientación apaisada) o 2 (para vertical). El valor predeterminado es 1.

El cambio entra en vigor inmediatamente después de escribir el mandato de CLI y pulsar la tecla Intro.

Sintaxis

store pdf-config [orientation | size]

Mandato show

show pdf-config [orientation | size]

store pdf-config multilanguage_support

Hay diferentes archivos de configuración del generador pdf estático para el idioma inglés (utilizado en la versión inglesa) y para el idioma C/J (utilizado en chino/japonés). Utilice este mandato de CLI para definir los fonts en el generador de PDF. El valor predeterminado es inglés. El idioma C/J es multilingüe.

Sintaxis

```
CLI> store pdf-config multilanguage_support
Current setting is Default

1  Default
2  Multi-language
Please select the option (1,2, or q to quit)
```

Mandato show

show pdf-config multilanguage_support

store populate_from_query_maxrecs

Establece el número máximo de registros que se pueden utilizar para rellenar los grupos y alias de una consulta.

Preste atención cuando establezca el número máximo de registros con este mandato de CLI. Si el valor es demasiado alto, es posible que los procesos de Cumplimentar grupo desde consulta estén incompletos. El umbral máximo es dinámico y depende de la carga del sistema y el uso de memoria. El valor más alto de este mandato de CLI está limitado a 200000.

Sintaxis

store populate_from_query_maxrecs 100000

Mandato show

show populate_from_query_maxrecs

store product gid

Establece el valor GID <n> exclusivo del producto.

Sintaxis

store product gid <n>

Mandato show

show product gid

store purge object

Establece la antigüedad (en días) en la que se depurarán los objetos no esenciales. Utilice el mandato show purge objects age para visualizar una tabla que muestra el índice, el nombre de objeto y la antigüedad de cada tipo de objeto para el que se mantiene una antigüedad de depuración. A continuación, utilice en el mandato el índice adecuado de dicha tabla para establecer la antigüedad de depuración.

Nota: El valor de número de días se establece en el valor predeterminado (90 días) cuando el tipo de unidad cambia de unidad gestionada/Gestor/unidad autónoma.

Sintaxis

store purge object age <index> <days>

Mandato show

show purge object age

Ejemplo

Presuponga que desea conservar un registro de sucesos durante 30 días. En primer lugar, emita el mandato show purge objects age para determinar el índice (no utilice la tabla, su lista puede ser diferente). A continuación, escriba el mandato store purge object.

CLI>show purge objects age

Nombre de índice, Antigüedad

1. Operaciones persistentes de gestión central, 7
2. Registro de sucesos de S-TAP, 14
4. Pruebas de asesoramiento, 7
5. Políticas temporales de gestión central, 7
6. Historial de cambios de S-TAP, 14
7. Información de autenticación de Kerberos, 1
8. Historial de comentarios, 60
9. Historial de comentarios local. 60
10. Historial gráfico de llamadas, 90

. . .

ok

CLI> **store purge object age 2 30**

ok

store quartz_thread_run

Este mandato de CLI es para el servicio de soporte técnico.

La Java™ Virtual Machine permite que la aplicación tenga varias hebras. La hebra es un fragmento de la ejecución del programa.

Utilice el mandato de CLI store quartz_thread_num para establecer el número de hebras que se pueden ejecutar al mismo tiempo.

Utilice este mandato para reducir conflictos cuando demasiadas hebras se ejecutan al mismo tiempo.

El mandato de CLI show quartz_thread_num CLI muestra el número de hebras del planificador Quartz que se ejecutan al mismo tiempo.

Sintaxis

store quartz_thread_run <number>

USO: store quartz_thread_num <number>, donde number es un número de 3 a 15, siendo 5 el valor predeterminado.

Mandato show

show quartz_thread_num

org.quartz.threadPoll.threadCount= 5

store remotelog

Controla el uso del registro remoto. Además de los mensajes del sistema, en el archivo syslog se pueden grabar las alertas de estadísticas y los mensajes de infracción de reglas de políticas (opcionalmente). Para cada combinación **facility.priority**, se puede dirigir los mensajes a un host específico. Este mandato también puede controlar el uso del registro remoto mediante un número de puerto opcional y puede designar un protocolo obligatorio (UDP o TCP). Este mandato funciona con cualquier implementación de syslog que soporte TCP.

Si habilita el registro remoto, asegúrese de que el host receptor tenga habilitada esta función (consulte la nota).

Sintaxis

store remotelog [help|add|clear] facility.priority host [número puerto opcional:protocolo obligatorio (UDP o TCP)]

Tabla 2. Parámetros de store remotelog

Parámetros	Descripción
help	Muestra los recursos y prioridades soportados.
add	Añade la combinación de facility.priority a la lista de mensajes que se han de enviar al host remoto especificado.
clear	Borra la combinación de facility.priority de la lista de mensajes que se envían al host especificado.
facility	Utilice daemon. La mayor parte de los mensajes que emite el dispositivo IBM Guardium proceden del recurso daemon.
priority	Puede ser uno de los siguientes valores: alert, all, crit, debug, emerg, err, info, notice, warning. Los códigos de gravedad de IBM Guardium para la correlación de alertas e infracciones son los siguientes: Gravedad de Guardium/Prioridad de syslog INFO / info LOW / warning MED / err HIGH / alert
host	Identifica el host que recibe esta combinación facility.priority.
número de puerto opcional	
protocolo obligatorio	UDP o TCP

Nota:

Para configurar el sistema receptor para que acepte el registro remoto, edite /etc/sysconfig/syslog en dicho sistema, de modo que incluya la opción -r. Por ejemplo:

```
SYSLOGD_OPTIONS=-r -m 0
```

A continuación, reinicie el daemon de syslog:

```
/etc/init.d/syslog  restart
```

El nombre del archivo syslog estándar en Linux es:

```
/var/log/messages
```

El criterio común requiere que se cifren todas las comunicaciones desde el sistema Guardium a un servidor syslog remoto. Las comunicaciones con el servidor syslog remoto no pueden estar en texto simple.

Mandatos de CLI

show remotelog

store remotelog ?

store remotelog add ?

store remotelog add encrypted

USO: store remotelog add encrypted <facility.priority> <host[:port]> <tcp|udp>

Recursos posibles: all auth authpriv cron daemon ftp kern local0 local1 local2 local3 local4 local5 local6 local7 lpr mail mark news security syslog user uucp

Prioridades posibles: alert all crit debug emerg err info notice warning

Nota:

Si desea enviar el mensaje de registro remoto cifrado al servidor, la configuración de rsyslog en el servidor debe aceptar mensajes cifrados.

El valor de cifrado en el cliente y el servidor solo funciona en modo TCP.

Cambio de una modalidad a otra en el mismo servidor remoto: Es necesario modificar el archivo de configuración para sincronizarlo con la modalidad designada y se debe reiniciar el servicio remoto.

Ejemplo

```
store remotelog add non_encrypted
store remotelog clear
g32.guard.swg.usma.ibm.com> show remotelog
*.*    @9.70.148.175:10514
```

Utilice el ejemplo para almacenar el certificado como ca.pem en /etc/pki/rsyslog/. Esto abre una nueva ventana que solicita al usuario que pegue el certificado.

```
store remote add encrypted all.all <dirección IP>:<número de puerto> tcp
```

Cifrado de syslog

Se pueden reenviar las alertas y los mensajes a un receptor syslog remoto, tal como un sistema SIEM. Este tráfico de mensajes se puede cifrar desde el recopilador o agregador para el receptor de syslog remoto.

Nota: El cifrado solo funciona en modalidad TCP. De forma predeterminada, el reenvío de syslog utiliza UDP, por lo tanto, si se requiere cifrado especifique TCP para el mandato de CLI store remotelog.

Antes de comenzar:

El procedimiento que se describe aquí se debe repetir en cada recopilador o agregador que envíe tráfico al host cifrado.

Es necesario el certificado que utiliza el servidor syslog remoto. Almacene este certificado en el sistema Guardium.

1. Tenga a mano al certificado público de la entidad emisora de certificados (CA) Verisign, Thwate, Geotrust, GoDaddy, Comodo, interno, etc.
2. Inicie sesión en CLI en el sistema Guardium individual desde el que envía el syslog cifrado. Antes de ejecutar el mandato, obtenga el certificado adecuado de la CA (en formato PEM) y copie el certificado en su portapapeles, incluidas las líneas de inicio y fin.
3. Escriba el mandato de CLI siguiente: store remotelog add encrypted daemon.all <dirección IP del host remoto cifrado>:<número de puerto del host remoto> tcp
   Nota: Este ejemplo utiliza daemon porque Guardium envía sus sucesos de aplicación utilizando daemon.
4. Se muestran las instrucciones siguientes:

   ```
   Pegue su certificado CA en formato PEM. Incluya las líneas BEGIN y END y, a continuación, pulse Ctrl-D.
   ```

   Pegue el certificado en formato PEM en la línea de mandatos y pulse **Ctrl-D**. Guardium tomará esta entrada y la almacenará como /etc/pki/rsyslog/ca.pem

   Se mostrará un mensaje para indicar si la operación store se ha realizado correctamente o no.

   Si se realiza correctamente, Guardium puede enviar tráfico cifrado al sistema remoto con la clave correcta.

5. Repita el procedimiento para cada recopilador y agregador que envíe tráfico syslog al host cifrado.

store s2c

Establece varios parámetros configurables para ADMINCONSOLE. Estos parámetros se utilizan para regular el tráfico de servidor a cliente (S2C).

Nota: Solo utilice este mandato de CLI cuando se lo indique el servicio técnico de IBM Guardium.

Valores mínimos y máximos:

ANALYZER_S2C_IGNORE = {0,1,2,3}

MAX_S2C_VELOCITY (K bytes/seg) - número >=0 y <= 2147483647

MAX_S2C_INTERVAL (seg) - número >=1 y <= 2147483647

Consulte también el mandato de CLI store throttle.

Sintaxis

store s2c

USO: store s2c ignore I maxrate M maxinterval T

donde 0<=I<=3 (nivel), 0<=M<=2147483647 (K/seg), y 1<=T<=2147483647 (segundos) O valor predeterminado de store throttle

store s2c ignore 3 maxrate 300 maxinterval 5007

La nueva configuración entra en vigor cuando se ejecuta el mandato de CLI restart inspection-core.

Mandato show

show s2c

Throttle S2C parameters (defaults):

Ignore: 0

Max rate: 999999

Max interval: 30

ANALYZER_S2C_IGNORE (0,1,2,3) - Activar o desactivar los mecanismos de regulación de s2c, en función de los casos de uso. Este distintivo está basado en bits. 0 = el mecanismo de regulación de s2c está desactivado. 1 = activa la función descrita en el escenario 1, 2 = activa la función descrita en el escenario 2. 3 = activa ambas funciones.

MAX_S2C_VELOCITY - velocidad máxima (K bytes/seg). Si se supera esta velocidad, el analizador debe enviar mandatos de CLI, ignorar sesión o ignorar respuesta de sesión, enviar una solicitud a S-TAP o sniffer.

MAX_S2C_INTERVAL - intervalo de tiempo en segundos (valor predeterminado 30 segundos) entre los posibles mandatos de CLI, ignorar sesión o ignorar respuesta de sesión, solicitudes.

Escenario 1

Sniffer empieza a recibir tráfico de S-TAP o de la red en medio de una consulta de gran tamaño. Dado que todos los paquetes entrantes son respuestas del servidor de BD, no se creará ninguna sesión nueva por parte del analizador y, por lo tanto, no se enviará ninguna información al registrador y al motor de reglas. Este tipo de tráfico no es útil para sniffer. Por otro lado, este tipo de tráfico puede crear una carga adicional para S-TAP y Sniffer. Un mecanismo de regulación ayuda a disminuir la carga de red de Sniffer y S-TAP enviando un mensaje de ignorar sesión desde el analizador, si la velocidad de S2C supera el valor de MAX_S2C_VELOCITY. Si por algún motivo S-TAP o el Sniffer de red no han resultado afectados, el analizador volverá a enviar la solicitud de ignorar sesión después del número de segundos de MAX_S2C_INTERVAL. Para poder activar este mecanismo de regulación, establezca el distintivo ANALYZER_S2C_IGNORE en 1.

Escenario 2

Si el tráfico de entrada tiene una velocidad de S2C alta (> MAX_S2C_VELOCITY), un mecanismo de regulación envía una solicitud de respuesta de ignorar sesión a S-TAP para las conexiones de base de datos locales en el si la velocidad de S2C supera el valor de MAX_S2C_VELOCITY. Si por algún motivo S-TAP o el Sniffer de red no han resultado afectados, el analizador vuelve a enviar la solicitud de respuesta de ignorar sesión después del número de segundos de MAX_S2C_INTERVAL. Para poder activar este mecanismo de regulación, establezca el distintivo ANALYZER_S2C_IGNORE en 2.

store sender_encoding

Utilice este mandato de CLI para codificar los mensajes de salida (correo electrónico y excepciones SNMP) en diferentes esquemas de codificación, en los que anteriormente todo estaba codificado en UTF8.

Por ejemplo, un cliente Guardium desea codificar todos los mensajes SNMP de salida en SJIS, una codificación japonesa alternativa.

Nota: Si falla conversión falla, debido a que (a) el esquema de codificación especificado no es válido, o (b) los caracteres que se deben codificar no se pueden representar en el esquema de codificación solicitado, el mensaje se enviará utilizando UTF8, que es el esquema de codificación predeterminado.

Sintaxis

store sender_encoding <str>,

donde str es la codificación con una longitud máxima de 16

Mandato show

show sender_encoding

store stap approval

Utilice esta función para impedir que los STAP no autorizados se conecten al dispositivo Guardium.

Si el valor es ON, los STAP no se pueden conectar hasta que se aprueben específicamente.

Si se conecta un STAP no aprobado, se desconectará inmediatamente hasta que lo autorice específicamente la dirección IP de dicho STAP.

Hay un informe predefinido para clientes aprobados, clientes TAP aprobados, disponible en el separador Supervisor diario.

Nota:

Se necesita una dirección IP válida, no el nombre de host.

El mandato de CLI, store stap approval, no funciona en un entorno con un equilibrador de carga de IP.

En un entorno gestionado central, después de añadir las IP a los STAP aprobados, hay un tiempo de espera asociado a la sincronización que puede durar hasta una hora. Una vez completada la sincronización, el estado de los STAP aprobados se muestra en verde en la GUI.

Sintaxis

store stap approval ON | OFF

Mandato show

show stap approval

Mandato GuardAPI

grdapi store_stap_approval

La nueva configuración entra en vigor cuando se ejecuta el mandato de CLI restart inspection-core.

store stap certificate

Almacena un certificado del host de S-TAP, (normalmente un servidor de bases de datos), en el dispositivo de IBM Guardium. Este mandato funciona exactamente igual que el mandato store certificate console, que se describe más adelante.

Sintaxis

store stap certificate

Se le solicitará lo siguiente:

Pegue su nuevo certificado de servidor en formato PEM.

Incluya las líneas BEGIN y END y, a continuación, pulse Ctrl-D.

Si todavía no lo ha hecho, copie el certificado de servidor en el portapapeles. Pegue el certificado en formato PEM en la línea de mandatos y pulse Ctrl-D. Se le informará de si la operación del mandato store se ha realizado correctamente o no.

Cuando haya terminado, utilice el mandato **restart gui** para reiniciar la GUI de IBM Guardium.

store stap network_latency

La verificación de S-TAP es una función con la que los clientes pueden verificar si un S-TAP está supervisando o no el tráfico de la base de datos. La función de verificación resulta afectada por el tráfico/latencia de la red. Dado que la latencia es diferente para cada cliente, es necesario un modo de listar y cambiar el valor predeterminado que utiliza la función de verificación.

Sintaxis

store stap network_latency

USO: store stap network_latency <N>

donde N es número mayor que 0 segundos.

El valor predeterminado es 5 segundos.

Si el número aumenta, se ralentiza el proceso de verificación de S-TAP.

Mandato show

show stap network_latency

store set_partitions_for_queries

Utilice este mandato de CLI para habilitar/inhabilitar la selección de particiones en las consultas.

Uso:

store set_partitions_for_queries <on|off>

store storage-system

store storage-system

Añade o suprime un tipo de sistema de almacenamiento para archivado o copia de seguridad del sistema.

Sintaxis

store storage-system <Centera | TSM> <backup | archive> <on | off>

Mandato show

show storage-system

Ejemplo

Presuponga que utiliza Centera para copias de seguridad del sistema, pero desea cambiar a un sistema TSM. Debe desactivar la opción de copia de seguridad de Centera (a menos que desee dejarla como otra opción) y activar la opción de copia de seguridad de TSM. En el ejemplo se resaltan los mandatos para llevar a cabo esta acción. Los mandatos show no son necesarios, solo son para fines ilustrativos.

CLI> show storage-system

RED :

CENTERA : copia de seguridad

TSM :

SCP : archivado y copia de seguridad

FTP : archivado y copia de seguridad

ok

CLI>store storage centera backup off

ok

CLI> store storage tsm backup on

ok

CLI> show storage-system

RED :

CENTERA :

TSM : copia de seguridad

SCP : archivado y copia de seguridad

FTP : archivado y copia de seguridad

ok

CLI>

store support state

Habilita (**on**) o inhabilita (**off)** el envío de alertas de correo electrónico a la dirección de correo electrónico de soporte, que se puede configurar utilizando el mandato **forward support email**. De forma predeterminada, el estado de soporte está habilitado (**on**) y la dirección de correo electrónico de soporte predeterminada es support@guardium.com.

Sintaxis

store support state <on | off>

Mandato show

show support state

store throttle

Este mandato de CLI almacena los parámetros de regulación. Después de especificar este mandato, debe emitir el mandato de CLI restart inspection-core para que los cambios entren en vigor.

Este mandato para filtrar (omitir) los paquetes de gran tamaño. La regulación tiene dos modalidades: Umbrales por sesión: Ignorar sesiones cuando se identifica una ráfaga suficientemente grande (duración configurable) de paquetes grandes (tamaño configurable) y detener la omisión de la sesión cuando el tráfico supera un umbral determinado (también configurable). Y Global: Ignorar todos los paquetes que superen un tamaño determinado (configurable) en todas las sesiones. Esta modalidad de regulación ignora un número excesivo de paquetes que no son de base de datos y cuyo tamaño es menor que el tamaño predefinido (resulta útil para clientes de VNC y otros tipos de tráfico de ruido blanco). Se utiliza para el tráfico de red a través del puerto SPAM o TAP de hardware. En el caso del tráfico S-TAP, solo el tráfico TCP capturado por PCAP. Consulte también el mandato de CLI store s2c.

Sintaxis

store throttle [default | size <s> interval <i> trigger <t> release <r>]

USO: store throttle size S interval I trigger T release R

donde 0<=S<=2^17 (bytes), 1<=I,T,R,<=2^31 (segundos)

O valor predeterminado de store throttle

Mandato show

show throttle

Parámetros de regulación:

Tamaño de paquete: 228000

Intervalo de tiempo: 604800

Nivel de desencadenante: 10000000

Nivel de release: 10000000

Parámetros

predeterminado: Escriba el valor predeterminado de palabra clave para restaurar los valores predeterminados (no se utilizan otros parámetros)). Los parámetros de regulación predeterminados no se regulan nunca.

s: El tamaño del paquete en bytes, con un máximo de 217 (131072).

Los parámetros restantes son en segundos, hasta un máximo de 231 (2147483648):

i - El intervalo de tiempo

t - El nivel de desencadenante

r- El nivel de release

Nota: Para restaurar los valores predeterminados del regulador, utilice el mandato de CLI, store throttle default.

store timeout

Establece el valor de tiempo de espera excedido de una sesión CLI o una sesión de servidor. El valor predeterminado es 600 segundos. Un tiempo de espera también cierra la sesión CLI.

Si el servidor de archivos se detiene debido a un tiempo de espera excedido, se muestra un mensaje similar al siguiente: `Aviso: Se ha detenido el servidor de archivos debido a un tiempo de espera excedido. Es posible que el archivo no se haya cargado por completo. Deteniendo el proceso.`

Utilice los mandatos de CLI, show timeout db_connection, para mostrar el valor de socketTimeout en el archivo de configuración, y el mandato store timeout db_connection <valor>, para establecer el valor del tiempo de espera. El valor debe ser mayor que 0. El valor predeterminado es 25000 segundos. Estos mandatos de CLI se utilizan en la gestión de las comunicaciones entre el Gestor central y la unidad gestionada cuando DNS no está configurado.

Sintaxis

store timeout cli_session <n>

store timeout fileserver_session <n>

store timeout db_connection <n>

Mandato show

show timeout cli_session 600

show timeout fileserver_session 600

show timeout db_connection 25000

store transfer-method

Establece el método de transferencia de archivos utilizado para la exportación de CSV/CEF. Para el archivo de exportación, es necesario utilizar el mandato de CLI, store transfer-method csv, para establecer el método de la transferencia. En la copia de seguridad/archivado, utilice el mandato de CLI, store transfer-method backup, para establecer el método de transferencia.

Sintaxis

store transfer-method <FTP | SCP>

Mandato show

show transfer-method

Nota: Los archivos que se envían desde un dispositivo IBM Guardium a otro (desde un recopilador a un agregador, por ejemplo) siempre se envían utilizando SCP.

store uid_chain_polling_interval

Establezca el intervalo para el sondeo de series UID con este mandato de CLI. La serie de UID es un mecanismo que permite a S-TAP (mediante K-Tap) rastrear la serie de usuarios generada antes de una conexión de base de datos.

Establezca el intervalo en 0 para desactivar el proceso de la serie de UID, con el fin de mejorar el rendimiento de la base de datos. Si el proceso de la serie de UID está desactivado, se omiten el cálculo de la serie de UID y la actualización de sesiones hijo.

Nota: Cuando se utiliza cualquier base de datos, la serie de UID no se registra para todas las sesiones si la sesión es muy corta.

Sintaxis

store uid_chain_polling_interval <N>

donde N es el tiempo en minutos (> = 1 minuto; el valor predeterminado es 2 minutos)

Establezca N = 0, para desactivar el proceso de la serie de UID

Mandato show

show uid_chain_polling_interval

store upd_session_end

Este mandato de CLI añade una opción para omitir la actualización de la hora de session_end.

Sintaxis

store upd_session_end [enable | disable]

Mandato show

show upd_session_end

store unit type

Utilice este mandato de CLI para establecer los atributos de tipo de unidad del dispositivo Guardium. Consulte la tabla Atributos de tipo de unidad para obtener una descripción de todos los atributos de tipo de unidad que se pueden visualizar mediante este mandato.

Sintaxis

store unit type [manager | standalone] [netinsp] [stap] [mainframe] [sink]

Utilice `store unit type sink` para conmutar desde la granularidad de la indicación de fecha y hora del tráfico DRDA recopilado desde 1 milisegundo a 1 microsegundo.

Mandato show

show unit type

Nota: Algunos de los atributos listados se establecen con el mandato store unit type y se borran con el mandato delete unit type. El atributo de agregador solo se puede establecer durante la instalación del software de IBM Guardium y no se puede modificar, a menos que se vuelva a instalar el software de IBM Guardium.

Atributos de tipo de unidad

En la siguiente tabla, se muestran los atributos de tipo de unidad del sistema Guardium que se pueden visualizar con el mandato show unit type. Excepto donde se indique, estos atributos se pueden establecer con el mandato store unit type y se pueden borrar con el mandato delete unit type.

Tabla 3. Atributos de tipo de unidad

Atributo	Descripción
mainframe	La unidad es un dispositivo de inspección de red de sistema principal (z/OS).
manager	Las funciones del gestor central están habilitadas para esta unidad.
netinsp	La inspección del tráfico de red está habilitada.
network route static	Elimina una línea de la tabla de direccionamiento estático
standalone	Gestión local (independiente de un gestor central)
stap	La unidad puede recibir datos de y gestionar agentes S-TAP y CAS.

unregister management

El mandato unregister restaura la configuración que se ha guardado cuando se ha registrado el dispositivo para la gestión central. Si esto ha sucedido en un release anterior del software de IBM Guardium, si se restaura la configuración sin aplicar un parche para que la configuración guardada esté en el nivel de release de software actual, se inhabilitará el dispositivo y pueden perderse todos los datos almacenados. Por lo tanto, no anule el registro de una unidad hasta que haya verificado que la configuración previa al registro esté en el nivel de release de software actual. Si no está seguro sobre cómo verificarlo, póngase en contacto con el soporte técnico antes de eliminar el registro de la unidad.

Sintaxis

unregister management

Notas:

- Este mandato se ha diseñado solo para casos de emergencia, cuando el gestor central no está disponible.
- Después de anular el registro utilizando este mandato, también debe anular el registro desde el Gestor central (desde la Consola de administración), dado que es el único modo de reducir el número de unidades gestionadas. El recuento de unidades gestionadas está autorizado por la clave de producto.

Tema principal: Visión general de CLI
Información relacionada:
Soporte y resolución de problemas de Guardium (vídeo)

Mandato de CLI diag

Utilice estos mandatos de CLI para acceder a programas de utilidad de resolución de problemas y mantenimiento a través de diag.

Utilice el mandato diag siguiendo las indicaciones del servicio de soporte técnico.

No hay ninguna función que se realice de forma habitual con este mandato. Cada entrada del menú principal se describe en un tema diferente (consulte Mandatos del menú principal).

Programas de utilidad de resolución de problemas y mantenimiento mediante DIAG:

- Esquema de arreglos del agregador: Traslada todas las tablas importadas que tienen un esquema más antiguo que el del agregador al esquema de nivel de arreglo más reciente del agregador (se ejecuta como un proceso de fondo y puede tardar varias horas en completarse). Nota: Es posible que en algunos escenarios (a) el agregador no tenga el último nivel de parche, o (b) algunas de las tablas importadas tengan el último nivel de parche, con lo cual no todas las tablas importadas tendrán el último nivel de parche.
- Mantenimiento del agregador: Un análisis completo y recuperación del agregador. Este programa de utilidad recupera los registros de AGG relacionados y los coloca en la carpeta de exportación diag, invoca el esquema de arreglos del agregador para sincronizar el esquema para todas las bases de datos, limpia el espacio de trabajo AGG y reinicia el proceso de fusión para asegurarse de que se realiza un análisis completo de todas las tablas importadas (se ejecuta como un proceso de fondo y puede tardar varias horas en completarse).
- Limpiar huérfanos estáticos en un agregador: Esta opción solo la debe utilizar el servicio de soporte técnico y únicamente en los casos en los que el tamaño de las tablas estáticas haya aumentado demasiado y sea necesario realizar una limpieza. Este programa de utilidad limpia todos los registros antiguos que ya no se utilizan.

Abrir el menú principal de diagnósticos

Para utilizar el mandato diag, siga el procedimiento descrito:

1. En el indicador de línea de mandatos, inicie sesión en Guardium con CLI.

   El usuario de Guardium que desee utilizar el mandato diag debe tener asignado un rol de administrador o de CLI. De forma predeterminada, el único usuario que tiene un rol de CLI es el usuario admin. El usuario con un rol de CLI o admin puede especificar el mandato diag, utilizar los mandatos de CLI unlock admin y unlock accessmgr y utilizar el mandato de CLI export audit-data sin restricciones. No es necesario que el usuario con un rol de CLI escriba el nombre de usuario y la contraseña de inicio de sesión de GUI ni debe pasar un control adicional de su rol.

   Si el usuario de Guardium que intenta utilizar la CLI, no tiene un rol de CLI o admin, no se iniciará la CLI. El accessmgr asigna los roles CLI y admin.

2. Después de iniciar la CLI, escriba el mandato diag (sin argumentos) en el indicador de línea de mandatos.
3. El usuario de Guardium que desee utilizar el mandato diag debe tener asignado un rol de diag en el sistema Guardium. De forma predeterminada, solo el administrador tiene asignado este rol. El acceso a diag se permite o no, en función de la asignación de rol de este usuario (solo se permite el acceso a diag si el usuario tienen el rol de diag). El accessmgr asigna los roles diag.
4. Se muestra el menú de mandatos principal. Realice una de las acciones siguientes para mover el cursor de selección de opciones, que en este ejemplo está seleccionando el primer elemento:
    - Escriba el número de entrada que desee (el cursor de selección va a la entrada seleccionada).
    - Utilice la tecla de flecha arriba o flecha abajo para seleccionar la entrada que desee.
5. Pulse la barra espaciadora, la tecla de flecha izquierda o la tecla de flecha derecha para mover el cursor de selección de mandatos en la pantalla (en este ejemplo está seleccionado el mandato OK).
6. Realice una acción seleccionando la opción adecuada en el área de visualización y, a continuación, realice una de las acciones siguientes:
    - Seleccione el mandato adecuado con el cursor de selección de mandatos y, a continuación, pulse la tecla Intro.
    - Pulse el mandato de acción adecuado.

Acerca de la salida de diag

El mandato diag crea la salida en dos directorios:

- .../guard/diag/current
- .../guard/diag/depot

Puede acceder a esta salida con el mandato de CLI fileserver. Consulte el mandato fileserver para obtener más información.

En las subsecciones siguientes se describe cada directorio.

Directorio .../guard/diag/current

La mayor parte de la salida de los mandatos diag se graba en formato de texto en el directorio actual. Para la mayor parte de los mandatos, este directorio incluye un archivo de salida diferente. Cada vez que ejecuta el mismo mandato, se añade la salida al archivo individual para dicho mandato. En el caso de un número pequeño de mandatos, se crea un archivo separado para cada ejecución que normalmente incluye una indicación de fecha y hora en el nombre de archivo.

Se recomienda que realice una limpieza después de cada sesión, de modo que en las sesiones posteriores no esté consultando la información antigua. Cuando empaqueta los archivos en un archivo comprimido individual (consulte el tema siguiente), se suprimen todos los archivos del directorio actual. De forma alternativa, puede utilizar el mandato Suprimir registros en el menú Gestión de salida para suprimir archivos individuales.

Los archivos del directorio actual son fáciles de identificar, ya que los nombres se crean a partir de los nombres de menús y de mandatos. Por ejemplo, si utiliza el mandato Resumen de archivo en el menú Consultas interactivas del sistema, se crea un archivo interactive_filesummary.txt en el directorio actual.

Si observa el directorio actual mientras se procesa un mandato, podrá ver un archivo temporal oculto con el mismo nombre que el que contendrá la salida de dicho mandato. El archivo temporal se elimina cuando se añade la salida al archivo de salida de mandato.

Directorio .../guard/diag/depot

Cuando empaqueta los archivos de salida de diag en el directorio como un archivo comprimido (por ejemplo, para enviarlo al servicio de soporte técnico de Guardium) el archivo se almacena en el directorio depot. El nombre de archivo tiene el formato diag_session_<dd_mm_hhmm>.tgz, donde la parte variable del nombre indica cuándo se ha creado. Por ejemplo, el nombre de un archivo creado a las 12:15 PM del 20 de mayo será el siguiente: diag_session_20_5_1215.tgz.

Después de exportar los archivos (consulte el tema Exportar archivos de registros), puede eliminarlos del directorio depot utilizando el mandato Suprimir registros del menú Gestión de salida.

1 Gestión de salida

Los mandatos de Gestión de salida controlan lo que se lleva a cabo con la salida generada por el mandato diag. Cada mandato de gestión de salida se describe por separado.

1.1 Finalizar y empaquetar sesión actual

Utilice este mandato para empaquetar todos los archivos de diagnóstico del directorio actual en un único archivo comprimido y eliminar estos archivos del directorio actual. Cuando entra este mandato, no recibe información indicando que se ha completado el mandato. Puede verificar que el mandato ha finalizado consultando el directorio depot. Cuando se completa el mandato, existe un nombre de archivo con el formato siguiente: <mm_dd_hhmm>.tgz, donde la parte variable del nombre es una indicación de fecha y hora, como se ha descrito anteriormente. Utilice el mandato Exportar archivos de registro del menú Gestión de salida para enviar el archivo a otro sistema.

1.2 Suprimir registros

Utilice este mandato para suprimir archivos del directorio actual o el directorio depot. (Para suprimir únicamente los archivos de sesión actuales, utilice el mandato Suprimir archivos de sesión actual). Cuando especifica este mandato, se muestra la estructura del directorio depot:

Puede ir a los directorios pulsando las teclas de flecha arriba y flecha abajo y la tecla Intro. Por ejemplo, seleccione ../ y pulse Intro para subir la selección un nivel en la estructura de directorios.

A continuación, puede seleccionar el directorio actual y pulsar Intro para desplazarse a la parte inferior de dicha carpeta y suprimir archivos individuales de salida de mandato. Tenga en cuenta que puede ir a otros directorios pero no puede suprimir archivos que no sean del directorio actual o del directorio depot.

Una vez seleccionado el archivo que desea suprimir, pulse Intro.

Atención: Se le solicitará que confirme la acción de suprimir

1.3 Exportar archivos de registro

Utilice este mandato para enviar un archivo del directorio depot a otro sitio. Para exportar un archivo:

1. Seleccione Exportar archivos de registro en el menú de gestión de salida principal. Se muestra el directorio depot.
2. Seleccione el archivo que ha de enviar o utilice las entradas ../ y ./ para subir o bajar por la estructura de directorios. (No obstante, tenga en cuenta que solo puede exportar los archivos del directorio depot).
3. Con el archivo a transferir seleccionado, pulse Intro.
4. Se le solicitará que seleccione FTP o salir. Seleccione FTP y pulse Intro.
5. Se le solicitará un nombre de host. Escriba el nombre de host del sistema receptor (o su dirección IP) y pulse Intro.
6. Se le solicitará un nombre de usuario. Escriba un nombre de cuenta de usuario para el sistema receptor y pulse Intro.
7. Se le solicitará una contraseña. Escriba la contraseña del usuario del sistema receptor.
8. Se le solicitará que identifique un directorio para recibir el archivo enviado en el sistema receptor. Escriba la vía de acceso relativa a la raíz ftp del directorio que contiene el archivo en el sistema receptor y pulse Intro.
9. Se le solicitará que confirme los detalles de la transferencia (el archivo que envía y su destino). Pulse Intro para realizar la transferencia o seleccione Cancelar y pulse Intro para volver a comenzar.
10. Se le notificará si la operación se ha realizado correctamente o no.

1.4 Suprimir archivos de sesión actuales

Utilice este mandato para suprimir los archivos creados durante la sesión actual.

1.5 Salir

Utilice el mandato Salir para regresar al menú principal.

2 Informes estáticos del sistema

Utilice el mandato Informes estáticos del sistema del menú principal para generar un conjunto de informes de gran tamaño.

1. Seleccione Informes estáticos del sistema en el menú principal. Se le notificará que el proceso se está ejecutando.
2. Una vez creado el informe, se muestra en el área de visualización. Tenga en cuenta que este es un informe largo y le puede resultar más fácil visualizar en un editor de texto, después de exportarlo a un sistema de escritorio.

   Utilice la flecha arriba y la flecha abajo para subir o bajar por el informe. Cuando haya terminado de ver el informe, pulse Intro para regresar al menú principal.

Visión general de los informes estáticos del sistema

Los subtemas siguientes proporcionan una descripción de los componentes principales de la salida de informes estáticos del sistema. Los fragmentos de salida que se muestran están pensados para ilustrar el tipo y el nivel de información que contiene el informe, y no para proporcionar una descripción detallada del contenido real, lo cual está fuera del ámbito de este documento.

Información de configuración del sistema

La salida de los informes estáticos del sistema describe la versión de build, los parches aplicados, el tiempo de actividad del sistema actual y el nombre del servidor:

```
Build version: 34e1eb12eb68ba76cb49028251c9a0d6  /opt/IBM/guardium/etc/cvstag
Patches:
2009/02/22 16:16:50: START Installation of 'Update 5.0'
2009/02/22 16:18:04: Installation Done - Successfully Installed

< lines deleted… >

Current uptime:
  09:03:43  up 6 days, 17:34,  1 user,  load average: 0.44, 0.50, 0.41
System nameservers:
192.168.3.20
DB nameservers:
192.168.3.20
Gateway: 192.168.3.1 (system) 192.168.3.1 (def)
```

Next, the file system information displays (shown partially):

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/hdc3             2.0G  1.1G  813M  58% /
/dev/hdc1              97M  9.2M   83M  10% /boot
none                  504M     0  504M   0% /dev/shm
/dev/hdc2              71G  1.2G   66G   2% /var
        total:    used:    free:  shared: buffers:  cached:
Mem:  1055199232 1041711104 13488128        0 63275008 186220544
Swap: 536698880 295432192 241266688
MemTotal:      1030468 kB
MemFree:         13172 kB

< lines deleted… >
```

Esto va seguido de información acerca del correo y los servidores SNMP configurados:

```
SMTP server: 192.168.1.7 on port 25 : REACHABLE
SMTP user: undef
SMTP password: undef
SMTP auth: NONE
SNMP trapsink: undef UNREACHABLE
SNMP trap community: undef
SNMP read community: undef
```

La sección final de la configuración del sistema describe la configuración de red de la unidad: dirección IP, nombre de host, nombre de dominio, etc:

```
eth0:                192.168.3.101  (system) 192.168.3.101 (def)
hostname:                        (system)  g1 (def)
domain:                            (system)  guardium.com (def)
```

```
mac address:      00:04:23:A7:77:F2  (MAC1)  00:04:23:A7:77:F2 (MAC2)
unit type:           548 Standalone STAP
```

Información de la base de datos interna

La siguiente sección principal de la salida de los informes estáticos del sistema incluye información acerca del estado de la base de datos interna y las hebras (solo se muestran algunas hebras del principio):

```
uptime 77097  seconds.
27  threads.
78545028  queries.
+------+------------+-----------------------------+---------+---------+------+-----------
| Id   | User       | Host                        | db      | Command | Time | State |
+-------------------------------------------------------------------------------------------
| 1137 | enchantedg | localhost                   | TURBINE | Sleep   | 26   |
| 1257 | enchantedg | localhost.localdomain:33587 | TURBINE | Sleep   | 0    |
| 1258 | enchantedg | localhost.localdomain:60409 | TURBINE | Sleep   | 7716 |
| 1259 | enchantedg | localhost.localdomain:48233 | TURBINE | Sleep   | 322  |

< lines deleted… >
```

La lista de hebras va seguida de un análisis del estado de la tabla.

Información del contenedor del servlet web

Las siguientes secciones de la salida de informes estáticos del sistema contiene información acerca del contenedor de servlets web (Tomcat):

```
================================================================================
Currently defined Tomcat port is 8443.
The TOMCAT daemon is running and listening on port(s): 8005 8443.
Currently OPEN ports
java run by tomcat on port *:8443

< lines deleted… >
================================================================================

These are the nanny latest actions:
May 19 14:13:09 guard nanny:[5528]: Also checking tomcat.
May 19 14:13:09 guard nanny:[5528]: Going for my initial nap.

< lines deleted… >

This is the TOMCAT command line:
  463 sh -c ps -o pid,cmd -e | grep Dcatalina.base
21917 grep Dcatalina.base.
```

Información del motor de inspección

La siguiente sección principal de la salida de los informes estáticos del sistema contiene información acerca del motor de inspección:

```
================================================================================
This is the SNIF (pid: 13036) command line:  13036 /opt/IBM/guardium/bin/snif.
This is the SNIF status:
Name:               snif
State:                R (running)
Tgid: 13036

< lines deleted… >
================================================================================

Current timestamp is 2009-05-20 11:56:41
This is the last timestamp at GDM_CONSTRUCT_INSTANCE: 2009-05-20 11:56:41
This is the last timestamp at GDM_EXCEPTION: 2009-05-20 11:56:41
This is the last timestamp at GDM_POLICY_VIOLATIONS_LOG: 2009-05-20 11:56:41

================================================================================

Snif buf usage at Fri May 20 11:56:44 2009:
100 204800 buffers out of 204800
126 connection used, 32642 unused, 0 dropped (sniffer), 9 ignored (analyzer)
0 bytes lost, 60 connections ended, 601752099 bytes sent, 579063 request sent
Dropped Packets: 0 buffer full, 0 too short, 451 ignored
 time now is 1116604603
Analyzer/Parser buffers size: 6 (66533) 0 (62902)
 ms-tsql-logger  0 (11331)
 syb-tsql-logger  0 (70)
 ora-tsql-logger  79 (67803)
 db2-sql-logger  0 (20544)

< lines deleted… >
```

Información de tablas IP

La siguiente sección principal incluye información sobre las tablas IP:

```
================================================================================
IPTABLES:
-------------
       tcp  --  192.168.2.0/24       192.168.1.0/24      tcp spts:1521:60000  set 0x23
       tcp  --  192.168.1.0/24       192.168.2.0/24      tcp dpts:1521:60000  set 0x22
< lines deleted… >
```

Información acerca de S-TAP

La siguiente sección principal contiene información acerca de S-TAP:

```
================================================================================
STAP:
----
    0     0 ACCEPT     tcp  --  *      *  0.0.0.0/0      0.0.0.0/0          tcp spt:9500
    0     0 ACCEPT     tcp  --  *      *  0.0.0.0/0      0.0.0.0/0          tcp dpt:9500
 2696  148K ACCEPT     tcp  --  *      *  0.0.0.0/0      0.0.0.0/0          tcp spt:16016
 2835  175K ACCEPT     tcp  --  *      *  0.0.0.0/0      0.0.0.0/0          tcp dpt:16016

< lines deleted… >
```

Información acerca del tráfico IP

La siguiente sección principal contiene información acerca del tráfico IP:

```
IP traffic statistics.
OUTPUT OF ETH0
Fri May 20 11:57:04 2012; ******** Detailed interface statistics started ********

*** Detailed statistics for interface eth0, generated Fri May 20 11:58:04 2009

< lines deleted… >

OUTPUT OF ETH1
Fri May 20 11:57:04 2012; ******** Detailed interface statistics started ********

*** Detailed statistics for interface eth1, generated Fri May 20 11:58:04 2009

Total:               82440 packets, 53892382 bytes
        (incoming: 82440 packets, 53892382 bytes; outgoing: 0 packets, 0 bytes)
IP:    82440 packets, 52632747 bytes
        (incoming: 82440 packets, 52632747 bytes; outgoing: 0 packets, 0 bytes)

< lines deleted… >
```

Información acerca de STDERR y STDOUT del motor

La siguiente sección contiene la última salida de mensajes de Sniffer:

```
Snif  STDERR:

< lines deleted… >

Snif STDOUT:
Fri_20-May-2009_04:04:35 : Guardium Engine Monitor starting
Fri_20-May-2009_04:14:37 : Guardium Engine Monitor starting
Fri_20-May-2009_04:24:38 : Guardium Engine Monitor starting

< lines deleted… >
```

Información acerca del directorio de importación

La siguiente sección lista el contenido del directorio de importación:

```
These are the contents of the importdir directory:
total 0
```

Información acerca de la actividad del agregador

Esta sección lista las actividades del agregador (el ejemplo no incluye ninguna):

```
================================================================================
This is the aggregator last activities:
```

Informe de auditoría

Esta sección lista la siguiente información de resumen (vea el ejemplo):

```
================================================================================
Range of time in logs: 01/14/10 13:12:26.348 - 01/18/10 12:48:01.073
Selected time for report: 01/14/10 13:12:26 - 01/18/10 12:48:01.073
Number of changes in configuration: 4   - changes to the audit configuration
Number of changes to accounts, groups, or roles: 0
Number of logins: 22    - logins into the machine - ssh and console
Number of failed logins: 114
Number of authentications: 22 - "su", etc.
Number of failed authentications: 5
Number of users: 2
Number of terminals: 18
Number of host names: 9
Number of executables: 7
Number of files: 0
Number of AVC's: 0
Number of MAC events: 0
Number of failed syscalls: 0
Number of anomaly events: 3
Number of responses to anomaly events: 0
Number of crypto events: 0
```

```
Number of keys: 0
Number of process IDs: 9173
Number of events: 98669
================================================================================
```

Informe de anomalías

Esta sección lista lo siguiente (vea el ejemplo):

```
================================================================================
# Date Time Type Exe Term Host AUID Event
================================================================================
1. 01/14/10 13:16:02 ANOM_PROMISCUOUS /usr/sbin/brctl (none) ? -1 8 -  this is expected
to appear - it means the bridge is listening to all traffic
```

Informe de autenticación

Esta sección lista lo siguiente (vea el ejemplo):

```
================================================================================
# Date Time Type Exe Term Host AUID Event
================================================================================
1. 01/14/10 13:13:22 tomcat ? console /bin/su yes 4
2. 01/14/10 13:16:44 tomcat ? console /bin/su yes 11
3. 01/14/10 13:16:44 tomcat ? console /bin/su yes 17
4. 01/14/10 13:16:45 tomcat ? console /bin/su yes 23
5. 01/14/10 13:16:48 tomcat ? console /bin/su yes 29
6. 01/14/10 13:22:29 tomcat ? ? /bin/su yes 155
7. 01/14/10 13:28:10 ? ? tty1 /bin/login no 252
8. 01/14/10 13:28:20 ? ? tty1 /bin/login no 254
```

Informe de inicio de sesión

Esta sección lista lo siguiente (vea el ejemplo):

```
================================================================================
# Date Time Type Exe Term Host AUID Event
================================================================================
1. 01/14/10 13:22:15 root 192.168.2.9 sshd /usr/sbin/sshd no 142
2. 01/14/10 13:22:15 root 192.168.2.9 sshd /usr/sbin/sshd no 143
3. 01/14/10 13:22:17 root 192.168.2.9 sshd /usr/sbin/sshd no 144
4. 01/14/10 13:22:17 root 192.168.2.9 sshd /usr/sbin/sshd no 145
5. 01/14/10 13:22:20 root 192.168.2.9 sshd /usr/sbin/sshd no 146
```

3 Consultas interactivas

Seleccione Consultas interactivas en el menú principal para abrir el menú de consultas interactivas. (Utilice la tecla de flecha abajo para ir al décimo elemento y ver todos los elementos de este menú).

Además de visualiza la información solicitada, cada mandato de consulta interactiva crea salida en un archivo de texto separado en el directorio actual). Consulte el tema Visión general para obtener información acerca de los archivos creados.

En las secciones siguientes se describe cada mandato.

3.1 Archivos modificados

Utilice el mandato Archivos modificados para ver una lista de los archivos que se han modificado antes o después de un número de días especificado.

1. Seleccione Archivos modificados en el menú de consultas interactivas. Se le solicitará el número de días. Escriba un número y pulse Intro.
2. Se le preguntará si le interesan los archivos que se han modificado antes o después de dicho número de días. Seleccione 1 o 2 y pulse Intro.
3. Se muestra la vía de acceso completa de cada archivo modificado. Tenga en cuenta que todos los datos no caben en el área de visualización, utilice las teclas de flecha arriba y flecha abajo para desplazarse por los datos. La posición actual del archivo se indica mediante un número. Las barras blancas del área de visualización indica que existen más datos con un signo más.

3.2 Listar carpeta

Utilice este mandato para listar el contenido de diferentes directorios.

1. Seleccione Listar carpeta en el menú de consultas interactivas.
2. Se le solicitará que seleccione un directorio. Seleccione un directorio y pulse Intro. Se muestra el directorio seleccionado. Recuerde que si ejecuta varios mandatos al mismo tiempo, los datos de cada ejecución del mandato se añade al archivo de texto individual para dicho mandato.
3. Pulse Intro o Salir cuando haya terminado.

3.3 Resumir carpeta

Utilice el mandato Resumir carpeta para ver la salida del mandato du (Uso de disco):

1. Seleccione Resumir carpeta en el menú de consultas interactivas. No hay solicitudes. Verá el uso de disco en diferentes directorios.
2. Utilice la flecha arriba y la flecha abajo para desplazarse por los directorios.
3. Pulse Intro o Salir cuando haya terminado.

3.4 Resumen de archivo y exportar

Utilice este mandato para listar un archivo de registro completo o una parte del mismo.

1. Seleccione Resumen de archivo en el menú de consultas interactivas.

2. Se le solicitará que seleccione un archivo. Utilice la flecha arriba y la flecha abajo para desplazar el cursor de selección al archivo que desea ver.
3. Pulse Intro o Aceptar.
4. Se le solicitará que seleccione el número de líneas que se han de visualizar. Realice su selección y pulse Intro.
5. Se le solicitará que escriba una serie de búsqueda opcional. Utilice este recuadro si busca un mensaje de registro concreto (puede especificar una expresión regular). De lo contrario, deje en blanco el recuadro y pulse Intro.
6. Siga las indicaciones y pulse Intro para aceptar, lo que significa que solo se mostrarán archivos exclusivos. De lo contrario, seleccione No y pulse Intro (se mostrarán todos los archivos).

   Tenga en cuenta que cuando se utiliza el estilo de resumen, las variables se sustituyen por el signo de almohadilla (#). En algunos datos de registro que contienen variables, tales como las direcciones IP o las fechas, las sustituciones pueden ser extensas.

3.5 Probar correo electrónico

Utilice este mandato para enviar un correo electrónico de prueba al servidor SMTP configurado.

1. Seleccione Probar correo electrónico en el menú de consultas interactivas.
2. Se le solicitará que seleccione un destinatario. Seleccione Personalizar y pulse Intro.
3. Se le solicitará una dirección de correo electrónico. Escriba una dirección de correo electrónico y pulse Intro. Se le informará sobre la salida de la operación. Tenga en cuenta que en la consola de administración, el enlace Probar conexión en el panel SMTP del panel de configuración del alertador solo prueba que esté configurado un puerto SMTP, no si el correo se ha entregado mediante dicho servidor. Puede utilizar este mandato para probar la entrega del correo electrónico sin tener que configurar y desencadenar una alerta de estadísticas o en tiempo real o una notificación del proceso de auditoría.

3.6 Probar SNMP

Utilice este mandato para probar una excepción SNMP en el servidor SNMP configurado.

1. Seleccione Probar SNMP en el menú de consultas interactivas.
2. Se le notificará la actividad y los resultados. Tenga en cuenta que en el panel de configuración del alertador, el enlace Probar conexión del panel SNMP solo prueba que esté configurado un puerto SNMP, no si se ha entregado una excepción mediante dicho servidor. Puede utilizar este mandato para probar la entrega de excepciones sin tener que configurar (y desencadenar) una alerta de estadísticas o en tiempo real o una notificación del proceso de auditoría.

3.7 Datos de informe de consulta

Utilice este mandato para ver la sentencia Select real que se está utilizando para un informe de consulta . Esto puede resultar útil se un informe escrito por el usuario genera una salida imprevista.

1. Seleccione Datos de informe de consulta en el menú de consultas interactivas.
2. Se le solicitar que realice una selección en lista de títulos de informes. Utilice la flecha arriba y la flecha abajo para seleccionar una entrada y pulse Intro. Cada entrada de esta lista es una entidad de informe. En primer lugar, se listan todos los informes predefinidos. Están numerados en un rango de 100-225 (para la versión 3.6.1 – es muy probable que aumenten incrementalmente en cada release, ya que se crean más informes predefinidos).

   Los informes escritos por el usuario se listan después de los informes predefinidos, comenzando por el número 20001 (para la versión 3.6.1).

   Se muestra la sentencia de selección del informe seleccionado.

3.8 Consultas GDM

Utilice este mandato para ver el recuento de las llamadas SQL observadas durante un intervalo de 100 segundos.

1. Seleccione Consultas GDM en el menú de consultas interactivas.
2. Se muestra un mensaje solicitando su paciencia. Selección Sí para continuar. La columna CMD_CT lista el número de llamadas SQL observadas desde los clientes especificados a los servidores especificados.
3. Pulse Intro cuando haya terminado de ver el informe.

3.9 Generar volcado de TCP

Utilice este mandato para crear un volcado de TCP. La salida de este mandato se graba en un archivo de mandatos únicamente y no en la pantalla. A diferencia de la mayor parte de los otros mandatos, se crea un archivo separado en el directorio actual para cada ejecución de este mandato. El nombre de archivo tiene el formato: tcpdump_<mmaaaa-hhmmss>, donde la variable es una indicación de fecha hora: mmaaaa indica el mes y el año y hhmmss indica las horas, minutos y segundos.

1. Seleccione Generar volcado de TCP en el menú de consultas interactivas.
2. Se le solicitará que seleccione una interfaz. Seleccione un puerto y pulse Intro.
3. Se le solicitará una dirección IP de filtro opcional. Si únicamente le interesa el tráfico de una dirección específica, escriba dicha dirección IP y pulse Intro. De lo contrario, pulse Intro.
4. Se le solicitará un número de puerto opcional. Si únicamente le interesa el tráfico de un puerto específico, escriba dicho número de puerto y pulse Intro. De lo contrario, pulse Intro.
5. Se le solicitará que seleccione el número de segundos de tráfico que se ha de capturar. Seleccione un número de segundos y pulse Intro.
6. Se le solicitará que pulse Intro para iniciar la recopilación de datos. Pulse Intro. Regresará al menú después del número de segundos especificado (aproximadamente).
7. Para ver los datos de volcado de TCP, seleccione el mandato Leer volcados de TCP o exporte el archivo (consulte Exportar archivos de registro en el menú de gestión de salida, descrito anteriormente).

3.10 Leer volcados de TCP

Utilice este mandato para visualizar un archivo de volcado de TCP creado anteriormente.

1. Seleccione Leer volcado de TCP en el menú de consultas interactivas.
2. Se le solicitará que seleccione un archivo. Los archivos de volcado de TCP se listan desde los más antiguos a los más recientes. El nombre de archivo tiene el formato: tcpdump_<mmddaa-hhmmss>, donde la variable es una indicación de fecha hora: mmddaa indica el mes, el día y el año y hhmmss indica las horas, minutos y segundos. Seleccione el archivo que desea ver y pulse Intro.
3. Se muestra el archivo seleccionado. Utilice la flecha arriba y la flecha abajo para desplazarse por la pantalla y pulse Intro cuando haya terminado.

3.11 Ver almacenamiento intermedio

Utilice este mandato para ver la actividad de los almacenamientos intermedios de Guardium:

1. Seleccione Ver almacenamiento intermedio en el menú de consultas interactivas. La visualización se actualiza cada segundo.
2. Pulse Ctrl-C para cerrar la visualización.

3.12 Programa de utilidad SLON

Utilice este mandato para ejecutar el programa de utilidad slon, que rastrea los paquetes. Normalmente, este mandato solo se ejecuta como lo indica el servicio de soporte técnico. La salida de este mandato no se graba en la pantalla. La salida de uno de los dos archivos de mandato se graba en el directorio actual para cada ejecución del mandato: apks.txt.<día_dd-mmm-aaaa_hh.mm.ss.ttt> O <día_dd-mmm-aaaa_hh.mm.ss.ttt>

Las partes variables de los nombres de archivos son indicaciones de fecha y hora. Por ejemplo, apks.txt.Fri_20-May-2011_08.52.00.789.

1. Seleccione el programa de utilidad Slon en el menú de consultas interactivas.
2. Seleccione la acción que se ha de realizar y pulse Aceptar. Las opciones son:

   (a) volcar información de reglas del analizador

   (f) filtrar paquetes del analizador según IP o máscara

   (p) volcar paquetes en apks.txt

   (l) volcar las solicitudes del registrador en requests.txt

   (m) volcar paquetes STAP (Seleccione la duración de la ejecución. Espere a que termine y consulte el archivo msg-dump en /var/log/guard/diag/current/tap/)

   (r) registrar el tráfico IPQ

   (s) volcar la información de máquina de estado

   (t) configurar parámetros de regulación

3. Independientemente de su selección, se le solicitará que seleccione el periodo de tiempo de la actividad. Seleccione un periodo de tiempo y pulse Intro.
4. Se le notifica que el programa se ejecutará durante el periodo de tiempo especificado y se le solicitará que pulse Intro. Pulse Intro y espere.
5. Cuando finaliza el proceso, se muestra un mensaje. Puede utilizar el mandato Resumen de archivo para ver la salida de este mandato. Dado que este mandato puede generar una gran cantidad de datos, es posible que desee exportar el archivo a otro sistema en el que pueda ver el contenido mediante un editor de texto. (Empaquete los datos de la sesión actual y exporte los registros, como se ha descrito anteriormente en esta sección).

3.13 Mostrar índices

Utilice este mandato para mostrar los índices de diferentes tablas internas:

1. Seleccione Mostrar índices en el menú de consultas interactivas.
2. Se le solicitará que seleccione una tabla. Seleccione una tabla y pulse Intro para visualizar los índices de dicha tabla.
3. Utilice la flecha arriba y la flecha abajo para desplazarse por la visualización. Pulse Intro cuando haya terminado.

3.14 Comprobación de S-TAP

Utilice este mandato para visualizar las definiciones de S-TAP y la información de tráfico:

1. Seleccione Comprobación de S-TAP en el menú de consultas interactivas.
2. El tipo de unidad del sistema se muestra en formato numérico. Pulse Intro.
3. Se le solicitará que seleccione el número de segundos para supervisar el tráfico de S-TAP. Utilice la flecha arriba y la flecha abajo para realizar una selección y pulse Intro.
4. Se le informa del periodo de tiempo de espera aproximado y se le solicita que pulse Intro. Pulse Intro.
5. Se muestran los informes de definiciones de S-TAP y tráfico del servidor. Pulse Intro cuando haya terminado de ver el informe.

3.15 Estado de enlace de la interfaz

Utilice este mandato para ver el estado de enlace de la interfaz.

1. Seleccione Estado de enlace de la interfaz den el menú de consultas interactivas.
2. Se muestra el estado de todas las interfaces. Utilice la flecha arriba y la flecha abajo para desplazarse por la visualización.
3. Pulse Intro cuando haya terminado. Tenga en cuenta que este mandato solo muestra el estado del enlace. Para ver la información de configuración de la interfaz, utilice el mandato de CLI show network interface all.

3.16 Mostrar datos de regulación

Utilice este mandato para ver los datos de regulación.

1. Seleccione Mostrar datos de regulación en el menú de consultas interactivas.
2. Pulse Intro y espere 3 segundos a las estadísticas de regulación.
3. Utilice la flecha arriba y la flecha abajo para desplazarse por la pantalla y pulse Intro cuando haya terminado.

3.17 Generar volcado TCP y slon

Utilice este mandato para crear un volcado de TCP y ejecutar el programa de utilidad slon, que rastrea los paquetes. Normalmente, este mandato solo se ejecuta como lo indica el servicio de soporte técnico. Consulte los temas individuales, Generar volcado de TCP y Programa de utilidad Slon.

3.18 Generar volcado de SSL

Utilice este mandato para crear un volcado de SSL.

1. Seleccione Generar volcado de SSL en el menú de consultas interactivas.
2. Seleccione una interfaz y pulse Aceptar. Escriba la dirección IP de filtro y pulse Aceptar. Escriba el número de puerto de filtro y pulse Aceptar.
3. Seleccione el periodo de ejecución y pulse Aceptar. Pulse Aceptar y espere el periodo de tiempo especificado para recopilar los volcados de TCP.
4. Si desea ver los volcados de SSL, pulse Aceptar.
5. Pulse Intro cuando haya terminado.

3.19 Ver historial de bash

Utilice este mandato para ver el historial de bash.

1. Seleccione Ver historial de bash en el menú de consultas interactivas.
2. Pulse Aceptar.
3. Utilice la flecha arriba y la flecha abajo para desplazarse por la pantalla y pulse Intro cuando haya terminado.

3.20 Generar volcado GDM_Error

Utilice este mandato para crear volcados GDM_ERROR.

1. Seleccione Generar volcados GDM_ERROR en el menú de consultas interactivas.
2. Pulse Aceptar y escriba la contraseña. Pulse Intro.
3. Utilice la flecha arriba y la flecha abajo para desplazarse por la pantalla y pulse Intro cuando haya terminado.

3.21 Preparar volcado de memoria de Tomcat

Cuando Tomcat tiene un primer error outOfMemory, realiza un volcado de memoria en /var/tmp/tomcat/tomcat.dmp. Utilice este mandato para comprimir, cifrar y mover este archivo a /var/log/guard/diag/tomcat/ para recuperarlo mediante fileserv.

1. Seleccione Generar volcado de memoria de Tomcat en el menú de consultas interactivas.
2. Pulse Aceptar.
3. Utilice la flecha arriba y la flecha abajo para desplazarse por la pantalla y pulse Intro cuando haya terminado.

3.22 Información de red ampliada

Pulse la opción Información de red ampliada, bajo consultas interactivas del sistema, para ver información de diagnóstico de red.

Ejemplo

SQLGuard Diagnostics

Network Parameters from ADMINCONSOLE_PARAMETER:

SYSTEM_NETMASK1: 255.255.255.0

SYSTEM_DOMAIN:

SYSTEM_DEFAULT_ROUTE:

SYSTEM_DNS1:

SYSTEM_DNS2:

SYSTEM_DNS3:

TOMCAT_IP:

MANAGER_IP:

HOST_MAC_ADDRESS:

SECOND_DEVICE:

3.23 Generar volcado de TCP rotatorio

Esta es una selección diferente a otras selecciones de diag, en la sección Generar TCP y Generar TCP y slon.

Para generar un volcado TCP rotatorio, escriba la dirección IP de filtro (deje en blanco para todas las IP). Escriba el número de puerto de filtro. En la pregunta, ¿Cuánto tiempo se ha de ejecutar?, si ya se está ejecutando el volcado de TCP rotatorio, seleccione la opción "Desactivar Rotación" o "Rotación" (Activada). Si selecciona rotación, añada el tamaño de archivo.

El volcado de TCP se guarda en /var/log/guard/tcp.bin1 y /var/log/guard.bin2 en rotación.

Vuelva a seleccionar el volcado TCP en rotación para detener el proceso loop_tcpdump.sh.

4 Realizar acciones de mantenimiento

Seleccione la opción Realizar acciones de mantenimiento del menú principal para abrir el menú de mantenimiento. Utilice estos mandatos únicamente siguiendo las instrucciones del servicio de soporte técnico. Normalmente no es necesario ejecutarlo de forma habitual.

4.1 Análisis de TURBINE (actualizar cardinalidad de índices)

Utilice este mandato para optimizar la cardinalidad de índices de la base de datos de Guardium interna. Se muestra una barra de progreso mientras se ejecuta la operación. Cuando se completa la operación, regresa al menú de mantenimiento.

4.2 Optimizar TURBINE (vuelve a crear índices, tarda más tiempo)

Utilice este mandato para analizar y volver a indexar la base de datos interna de Guardium.

1. Seleccione Optimizar TURBINE (cardinalidad de índices) en el menú de mantenimiento. Se muestra una barra de progreso mientras se ejecuta la operación. Cuando se completa la operación, regresa al menú de mantenimiento.

4.3 Borrar espacio de disco

Utilice este mandato para borrar el espacio de disco no utilizado. Cuando se completa el procedimiento, regresa al menú de mantenimiento.

1. Seleccione Borrar espacio de disco en el menú Mantenimiento. Se le solicitará que seleccione un directorio.
2. Seleccione el directorio del que desea eliminar archivos. Se lista el contenido del directorio y se le solicita que confirme que desea eliminar todos los archivos.
3. Cuando se completa la operación, regresa al menú de mantenimiento.

4.4 Mantenimiento de RAID

Utilice este mandato únicamente siguiendo las instrucciones del servicio de soporte técnico. Este mandato proporciona acceso al menú de gestión del programa de utilidad del controlador RAID, que se puede utilizar para ver el estado de las unidades RAID. Si el sistema no tiene un controlador RAID, se muestra un mensaje de error si selecciona este mandato. Debe tener mucho cuidado cuando utilice el programa de utilidad del controlador RAID, ya que algunas de las funciones que se proporcionan pueden borrar toda la información del disco.

4.5 Programa de utilidad de depuración de aplicaciones

Utilice este mandato para activar o desactivar la depuración. Se le solicita que habilite o inhabilite el registro o que restaure los valores predeterminados del sistema.

4.6 Modificar umbral de vigilancia de TURBINE

Utilice esta opción para cambiar el límite de tiempo de espera de consultas largas.

4.7 Forzar inicio de MySQL irrecuperable

Utilice esta opción cuando se lo indique el servicio de soporte técnico.

4.8 Transferencia de copias de seguridad y recuperación del sistema

Utilice este mandato para restaurar una versión de copia de seguridad de la base de datos interna. Se le solicita que confirme la operación.

4.9 Nivel de registro de Tomcat

Utilice este mandato para seleccionar el nivel de depuración de componentes. Seleccione una de las opciones siguientes:

Clasificador, Nivel de datos, Seguridad, Flujo de trabajo u Otros.

Seleccione Clasificador para seleccionar las opciones de nivel de depuración: ERROR, WARN, INFO, DEBUG, ALL.

Seleccione DLS (seguridad de nivel de datos), Workflow u Otros (entrada de texto) para seleccionar las opciones de nivel de depuración: ERROR, WARN, INFO, DEBUG, ALL.

Si elige Otros (entrada de texto separado mediante ','), escriba los componentes válidos (dls, workflow, audit, customtable, gui, other, job).

4.10 Mantenimiento del agregador

Análisis completo y recuperación del agregador. Este programa de utilidad recupera los registros de AGG relacionados y los coloca en la carpeta de exportación diag, invoca el esquema de arreglos del agregador para sincronizar el esquema de todas las bases de datos, limpia el espacio de trabajo AGG y reinicia el proceso de fusión para asegurarse de que se realiza un análisis completo de todas las tablas importadas (se ejecuta como un proceso de fondo y puede tardar varias horas en completarse).

4.11 Esquema de arreglos del agregador

Traslada todas las tablas importadas al esquema de nivel de arreglo más reciento (se ejecuta como un proceso de fondo y puede tardar varias horas en completarse).

4.12 Limpiar huérfanos estáticos

Esta opción solo la debe utilizar el servicio de soporte técnico y únicamente en los casos en los que el tamaño de las tablas estáticas haya aumentado demasiado y sea necesario realizar una limpieza. Este programa de utilidad limpia todos los registros antiguos que no tienen asociada ninguna instancia. Se muestra un mensaje de progreso durante el proceso de la operación Limpiar huérfanos estáticos (lo utiliza el recopilador o el agregador).

5 Salir a CLI

Seleccione Salir a CLI en el menú principal. Pulse Intro para cerrar el mandato diag y volver a la interfaz de línea de mandatos.

Tema principal: Visión general de CLI

Mandatos de CLI de manejo de archivos

Utilice estos mandatos para la copia de seguridad y restauración de la información del sistema. Muchas de estas tareas se pueden realizar desde la interfaz de usuario de Guardium.

Acerca de los nombres de archivo de datos archivados

Cuando se archivan los datos de Guardium (o se exportan a un agregador), existe un archivo diferente para cada día de datos. En función de cómo se haya configurado la operación de exportar/depurar o archivar/depurar, es posible que tenga muchas copias de datos exportados del mismo día. Nombres de los archivos de datos de archivado y exportación tienen el mismo formato:

<secuenciadías>-<nombrehost.dominio>-w<indicación_fecha_ejecución>-d<fecha_datos>.dbdump.enc

secuenciadías es un número que representa la fecha de los datos archivados como el número de días desde el año 0. Se muestra la misma fecha con el formato aaaa-mm-dd en la parte fecha_datos del nombre.

nombrehost.dominio es el nombre de host del dispositivo Guardium en que se ha creado el archivo, seguido de un carácter de punto y el nombre del dominio.

indicación_fecha_ejecución es la fecha en que se han archivado o exportado los datos, con el formato aaaammdd.hhmmss.

fecha_datos es la fecha de los datos archivados con el formato aaaa-mm-dd.

Por ejemplo: 732423-g1.guardium.com-w20050425.040042-d2005-04-22.dbdump.enc

backup config

Estos mandatos realizan una copia de seguridad y restauración de la información de las tablas de administración internas. El mandato backup config almacena los datos en el directorio /media/backup. El mandato backup config elimina la licencia y otra información específica de la máquina. El mandato backup system proporciona una copia de seguridad más completa de la configuración y de todo el sistema.

Sintaxis

backup config

restore config

backup system

Este tema se aplica a las operaciones de copia de seguridad y restauración de la base de datos interna de Guardium. Puede realizar una copia de seguridad o restauración únicamente de la información de configuración o de todo el sistema (datos más configuración del sistema, excepto los archivos de claves secretas compartidos, cuya copia de seguridad y recuperación se hace por separado, consulte los mandatos de copia de seguridad de archivos de clave de copia de seguridad y de restauración de archivos de clave del agregador). Estos mandatos detienen todos los motores de inspección y servicios web y los reinician cuando finaliza la operación.

Antes de restaurar un archivo, asegúrese de que el dispositivo tenga el secreto compartido del sistema para el sistema que ha creado el archivo, de lo contrario no podrá descifrar la información. Consulte la sección Acerca del secreto compartido del sistema en la guía de administración de Guardium.
Nota: La restauración del sistema se lleva a cabo en el mismo nivel de parche que la copia de seguridad del sistema. Por ejemplo, si un cliente ha realizado la copia de seguridad del sistema cuando estaba en la versión 7.0, parche 7 y, a continuación, desea restaurar esta copia de seguridad en un dispositivo recién compilado, en primer lugar, debe instalar la versión 7.0, parches 1 a 7 en el dispositivo y únicamente después de instalarlos debe restaurar el archivo.
Hay dos mandatos implicados en el proceso de restauración:

- import file, que devuelve un archivo de copia de seguridad archivado al sistema
- restore system, que restaura el sistema desde un archivo de seguridad que previamente ha devuelto una ejecución del mandato import file.

En todos los mandatos backup, import y restore, se le solicitará que proporcione una combinación de los elementos siguientes, en función de los sistemas de almacenamiento configurados y del tipo de operación de restauración. Responda a cada solicitud, según corresponda a su operación. La tabla siguiente describe la información que se le puede solicitar.

Nota:

Se guarda una copia de la transferencia de archivos SCP/FTP/TSM/Centera, independientemente de si se ha realizado correctamente o no la transferencia. Dado que algunos archivos pueden tardar horas en volver a generarse (por ejemplo, la copia de seguridad del sistema), es importante para el usuario tener preparada una copia disponible (sobretodo si falla la transferencia de archivos). Solo se retiene una copia de cada tipo de archivo (archivado/copia de seguridad del sistema/copia de seguridad de configuración/etc).

La copia de seguridad del sistema copia la licencia actual, la calibración y el número de orígenes de datos y, a continuación, realiza la copia de seguridad de los datos. La restauración del sistema restaura los datos y, a continuación, restaura la licencia, la calibración y el número de orígenes de datos. Esta secuencia se aplica a la restauración del sistema habitual. Si restaura desde un sistema anterior, es necesario volver a configurar la licencia, la calibración y el número de orígenes de datos.

Cuando configura las copias de seguridad, un valor de cero '0' para el número de puerto indica que se está utilizando el puerto predeterminado para dicho protocolo y no es necesario ningún cambio.

Tabla 1. backup system

Elemento	Descripción
SCP, FTP, TSM, Centera, Snapshot	Seleccione el método que se ha de utilizar para transferir el archivo. Solo se muestran TSM y Centera si se han habilitado estos métodos de almacenamiento (consulte el mandato store storage-method)
Data o Configuration	Seleccione Configuración solo para las copias de seguridad de información de configuración y definiciones o seleccione Datos para la copia de seguridad de datos junto con la información de configuración.
restore from archive o restore from backup	Seleccione restore from archive para restaurar los datos archivos archivados o seleccione restore from backup para restaurar la información de configuración.
normal o upgrade	Si restaura desde la misma versión de software de Guardium, seleccione norma. Si restaura la información de configuración después de una actualización de software del dispositivo Guardium, seleccione upgrade.
host	El host remoto del archivo de copia de seguridad.
remote directory	El directorio del archivo de copia de seguridad. Para FTP, el directorio es relativo al directorio raíz de FTP para la cuenta de usuario FTP utilizada. Para SSH, la vía de acceso del directorio ha de estar completa. Para los servidores Windows SSH, utilice nombres de vías de acceso de estilo Unix con barras inclinadas, en lugar de barras invertidas como en Windows.

Elemento	Descripción
username	El nombre de la cuenta de usuario que se ha de utilizar para la operación (en operaciones de copia de seguridad, este usuario debe tener permiso de escritura/grabación para el directorio especificado). **Nota:** En Windows, se acepta un usuario de dominio con el formato dominio\usuario
password	La contraseña del nombre de usuario.
file name	El nombre de archivo del archivo de archivado o copia de seguridad. Consulte los nombres de archivos de datos de archivado. Puede seleccionar varios archivos utilizando el carácter comodín * en el nombre del archivo. Se permite el uso del carácter comodín * en los métodos de transferencia FTP, SCP y Snapshot. No se permite el uso del carácter comodín * en los métodos de transferencia TSM o Centera.
Centera server	Escriba el nombre del servidor Centera. Si utiliza archivos PEA, utilice el formato siguiente: <Nombre host/IP>? <nombre de archivo PEA completo>, por ejemplo: 128.221.200.56?/var/centera/us_profile_rwqe.pea.txt
Centera clipID	En una operación de restauración de Centera, la dirección de contenido que devuelve la operación de copia de seguridad. Por ejemplo: 6M4B15U4JM4LBeDGKCPF9VQO3UA

Una vez se ha proporcionado toda la información necesaria para la operación de copia de seguridad o restauración, se muestra una serie de mensajes que informan acerca de los resultados de la operación. Por ejemplo, en una operación de restauración del sistema, los mensajes serán similares a los siguientes, en función del tipo de restauración y el método de almacenamiento utilizados:

```
gpg: Signature made Thu Feb 22 11:38:01 2009 EST using DSA key ID 2348FF9E gpg: Good signature from "Backup Signer
<support@guardium.com>" Proceeding to shutdown services Proceeding to startup services Safekeeping admin.xreg Safekeeping
client.xreg Safekeeping controllers.xreg Safekeeping controls.xreg Safekeeping guardium-portlets.xreg Safekeeping local-
portlets.xreg Safekeeping local-security.xreg Safekeeping local-skins.xreg Safekeeping media.xreg Safekeeping portlets.xreg
Safekeeping security.xreg Safekeeping skins.xreg guard_sniffer.pl -reorder Recovery procedure was successful. ok
```

Impedir que los scripts de copia de seguridad y archivado llenen /var

El proceso de seguridad comprueba si hay espacio en /var antes de que se produzca una error de ejecución. Este proceso también avisa al usuario si no hay espacio suficiente para la copia de seguridad.

El proceso de archivado comprueba el tamaño de las tablas estáticas y se asegura de que haya espacio suficiente para crear el archivo de archivado.

Se registra un error en el archivo de registro y la GUI si la copia de seguridad supera el 50%

Ejemplo:

```
ERROR: /var backup space is at 60% used. Insufficient disk space for backup. CLI> backup system     1. DATA     2. CONFIGURATION
Please enter the number of your choice: (q to quit) 1      1. SCP     2. CONFIGURED DESTINATION  Enter the number of your choice:
(q to quit) 2 Make sure destination is configured in the GUI under the System Backup option Please wait, this may take some time.
```

backup profile

Utilice este mandato para mantener los datos del perfil de copia de seguridad (mecanismo de parche).

El archivo de copia de seguridad se copia en el destino, según el perfil de copia de seguridad. Si el parámetro que indica si ha de conservar el archivo de copia de seguridad es "1", Y hay suficiente espacio en disco, el archivo de copia de seguridad se conserva en el sistema; de lo contrario, se elimina.

Se deben rellenar todos los campos, host de destino de copia de seguridad, directorio de destino de copia de seguridad, usuario de destino de copia de seguridad y contraseña de destino de copia de seguridad.

Sintaxis

show backup profile

Ejemplo

```
patch backup flag is 1    patch backup automatic recovery flag is 1    patch backup dest host is    patch backup dest dir is
patch backup dest user is    patch backup dest pass is    ok
```

Sintaxis

store backup profile

Ejemplo

```
Do you want to set up for automatic recovery? (y/n)    Enter the patch backup destination host:    Enter the patch backup
destination directory:    Enter the patch backup destination user:    Enter the patch backup destination password:
```

export audit-data

Exporta los datos de auditoría a partir de la fecha especificada (aaaa-mm-dd) desde diferentes tablas de Guardium internas a un archivo comprimido. Los datos desde la fecha especificada se almacenarán en un archivo comprimido en el directorio /var/dump. El archivo creado se identificará en los mensajes que genera el sistema. Consulte el ejemplo. Utilice este mandato únicamente siguiendo las instrucciones del servicio de soporte de Guardium.

Nota: Solo los usuarios con el rol de administrador pueden ejecutar este mandato.

Sintaxis

export audit-data <aaaa-mm-dd>

Ejemplo

```
If you enter the audit-data command for the date 2005-09-16, a set of messages similar to the following will be created: CLI>
export audit-data 2005-09-16 2005-09-16 Extracting  GDM_ACCESS  Data ... Extracting  GDM_CONSTRUCT  Data ... Extracting
 GDM_SENTENCE  Data ... Extracting  GDM_OBJECT  Data ... Extracting  GDM_FIELD  Data ... Extracting  GDM_CONSTRUCT_TEXT  Data ...
Extracting  GDM_SESSION  Data ... Extracting  GDM_EXCEPTION  Data ... Extracting  GDM_POLICY_VIOLATIONS_LOG  Data ... Extracting
 GDM_CONSTRUCT_INSTANCE  Data ... Generating tar file ...  /var/csvGenerationTmp ~ GDM_ACCESS.txt GDM_CONSTRUCT.txt
GDM_CONSTRUCT_INSTANCE.txt GDM_CONSTRUCT_TEXT.txt GDM_EXCEPTION.txt GDM_FIELD.txt GDM_OBJECT.txt GDM_POLICY_VIOLATIONS_LOG.txt
GDM_SENTENCE.txt GDM_SESSION.txt ~ Generation completed, CSV Files saved to /var/dump/732570-supp2.guardium.com-w20050919110317-
d2005-09-16.exp.tgz ok
```

Los datos de cada tabla de base de datos interna mencionada se graban en un archivo de texto, con formato CSV. El nombre del archivo termina con exp.tgz y el resto del nombre se crea como se describe en Acerca de nombres de archivos de datos archivados.

Puede utilizar el mandato export file para transferir este archivo a otro sistema.

delete audit-data

Utilice este mandato únicamente siguiendo las instrucciones del servicio de soporte de Guardium. Este mandato se utiliza para eliminar los archivos de datos de auditoría comprimidos. Se le solicita que escriba un número de índice para identificar el archivo que se ha de eliminar. Consulte la sección Acerca de nombres de archivos de datos archivados para obtener información acerca de cómo se crean los nombres de archivos de datos archivados.

Se le solicita que identifique el archivo que se va a eliminar.

Sintaxis

delete audit-data

show audit-data

Utilice este mandato para visualizar los archivos que se han creado al ejecutar el mandato de CLI, export audit-data. Para obtener más información acerca de los archivos de datos de auditoría, consulte export audit-data.

Sintaxis

show audit-data <aaaa-mm-dd>

export file

Este mandato exporta un nombre de archivo individual desde el directorio /var/IBM/Guardium/data/dump, /var/log o /var/IBM/Guardium/data/importdir.

Utilice este mandato únicamente siguiendo las instrucciones del servicio de soporte de Guardium. Para exportar datos de Guardium a un agregador o para archivar datos, utilice los mandatos del menú adecuado del panel de la consola de administración.

Sintaxis

export file </vía_acceso_local/nombrearchivo> <usuario@host:/vía_acceso/nombrearchivo>

vía_acceso_local debe ser una de las siguientes: /var/IBM/Guardium/data/dump, /var/log o /var/IBM/Guardium/data/importdir

fileserver

Utilice este mandato para iniciar un servidor de archivos basado en HTTPS que se ejecuta en el dispositivo Guardium. Este recurso está diseñado para facilitar la transferencia de parches a la unidad o para descargar la información de depuración desde la unidad. Cada vez que se inicia este recurso, suprime los archivos del directorio al que transfiere los parches.

Nota: Cualquier operación que genere un archivo al que accederá fileserver debe haber finalizado antes de que se inicie fileserver, de modo que el archivo esté disponible para fileserver.

Sintaxis

fileserver [`https://ip address:8445`] [`duration`]

`ip address` es una parámetro opcional que permite acceder a fileserver desde la dirección IP indicada. De forma predeterminada, (sin el parámetro), el acceso está restringido a la dirección IP del cliente SSH que ha iniciado fileserver.

`duration` es un parámetro opcional que especifica el número de segundos que está activo fileserver. Después del número de segundos especificado, fileserver concluye automáticamente. La duración puede ser cualquier número de segundos entre 60 y 3600.

En el caso de una configuración de seguridad en la que se redirigen las sesiones del navegador a través de un servidor proxy, la dirección IP del cliente de fileserver no será la misma que la del cliente SSH que ha iniciado fileserver. En su lugar, el cliente de fileserver tendrá la dirección IP del servidor proxy, y esta dirección debe pasar el parámetro `ip address` opcional. Para buscar la dirección IP del proxy, consulte los ajustes del navegador o las direcciones IP del cliente que se muestran en el informe Inicios de sesión en Guardium de la interfaz del Supervisor de Guardium.

Ejemplo

Para iniciar el archivo, escriba el mandato fileserver:

CLI> fileserver <dirección ip> <duración>

Iniciando el servidor de archivos. Puede encontrarlo en https://(nombre de dispositivo):8445

Pulse Intro para detener el servidor de archivos.

Abra el servidor de archivos en una ventana del navegador y realice una de las acciones siguientes:

- Para subir un parche, pulse Subir un parcha y siga las instrucciones.
- Para descargar los datos del registro, pulse Registros Sqlguard, vaya al archivo que desee y descargue del mismo modo que cualquier otro archivo.

Cuando haya terminado, regrese a la sesión CLI y pulse Intro para finalizar la sesión.

Cómo acceder a los scripts VA y de titularidad mediante fileserver

Instrucciones

En CLI, ejecute "fileserver <IP de su escritorio> 3600"

Asesoramiento de vulnerabilidades:

Abra un navegador y vaya a: https://<appliance ip>/log/debug-logs/gdmmonitor_scripts/

Seleccione el archivo que coincida con su tipo de base de datos

Titularidades:

Abra un navegador y vaya a: https://<ip dispositivo>/log/debug-logs/entitlemnts_monitor_role/

Seleccione el archivo que coincida con su tipo de base de datos

import file

Consulte backup config y restore config.

En el mandato de CLI import file puede utilizar el comodín * para el nombre de archivo en el método, scp, ftp e instantánea.

Sintaxis

import file

import tsm config

Sube un archivo de configuración del cliente de TSM al dispositivo Guardium. Debe hacerlo antes de realizar cualquier operación de archivado o copia de seguridad utilizando TSM. Siempre tendrá que subir un archivo dsm.sys y, si ese archivo incluye varias secciones servername, también tendrá que subir un archivo dsm.opt. Para obtener información sobre cómo crear estos archivos, consulte al administrador de TSM de su empresa.

Se le solicitará una contraseña para la cuenta de usuario en el host especificado.

Sintaxis

import tsm config <usuario@host:/path/[dsm.sys | dsm.opt]>

Parámetros

usuario@host - Cuenta de usuario para acceder al archivo en el host especificado.

/path/[dsm.sys | dsm.opt] - Nombre de archivo con vía de acceso completa del archivo que se ha de importar.

Nota: Cuando se configura TSM en cada recopilador, si la configuración inicial falla, se produce un error de notificación que indica que el archivo de prueba no se ha podido enviar. Si se inicia sesión en el recopilador como root y, a continuación, se ejecuta un mandato de archivado dsmc en el servidor TSM, el archivo TSM, con las mismas credenciales, se ejecuta correctamente. Si regresa a la GUI y se configura las mismas opciones anteriores, la configuración también se realiza correctamente.

Si tsm config tiene passwordaccess=generate, la contraseña que se almacena en un archivo local es sought. El usuario root debe ejecutar el mandato dsmc una vez para crear este archivo de contraseña local.

Después de subir el archivo tsm config, si tsm config tiene una solicitud passwordaccess igual a generate, significa que se ha establecido passwordaccess para que se genere.

```
¿Desea ejecutar un mandato dsmc ahora para asegurarse de que la contraseña se establezca localmente (y/n)?     Si la respuesta es
y, ejecute un mandato "dsmc query options>>/dev/null", que solicitará la contraseña al usuario.
```

import tsm property

Utilice este mandato de CLI para subir un archivo a /opt/tivoli/tsm/client/ba/bin/guard_tsm.properties.

El tamaño del archivo debe ser 1K.

Sintaxis

import tsm property user@host:file

Este mandato subirá el archivo de entrada a /opt/tivoli/tsm/client/ba/bin/guard_tsm.properties

restore config

Estos mandatos realizan una copia de seguridad y restauración de la información de las tablas de administración internas. El mandato backup config almacena los datos en el directorio /media/backup. El mandato backup config elimina la licencia y otra información específica de la máquina. El mandato backup system proporciona una copia de seguridad más completa de la configuración y de todo el sistema.

Cuando restaura una configuración, debe restaurar una copia de seguridad de la misma versión y nivel de parche que la del dispositivo original en que se ha creado la copia de seguridad.

Sintaxis

backup config

restore config

restore db-from-prev-version

Este mandato toma una copia de seguridad del sistema de un pasado inmediato (los datos de copia de seguridad se deben proporcionar, la copia de seguridad de la configuración es opcional) y realiza una restauración en un sistema más reciente. Esto incluye la actualización de datos, portlets, etc.

Realice una copia de seguridad del sistema completa antes de actualizar el sistema Guardium. Si por algún motivo falla la actualización y la máquina deja de poder utilizarse, en lugar de intentar arreglar y volver a ejecutar la actualización, vuelva a crear la máquina como el sistema más reciente, configurando este sistema más reciente únicamente con la información de red básica (IP, resolucionador, ruta, nombre de host del sistema y dominio).

Como resultado será el sistema más reciente con los datos y la personalización (si se ha proporcionado un archivo de configuración) del sistema anterior.

En primer lugar, intente realizar una actualización normal desde el sistema anterior al sistema más reciente. Si no se ejecuta correctamente, utilice la copia de seguridad como método alternativo para la actualización desde el sistema anterior al sistema más reciente.

Nota: Los datos más antiguos que se restauran en el agregador (no en el centro de investigación), y fuera del periodo de fusión, no se verán hasta que se cambie el periodo de fusión y se vuelva a ejecutar el proceso de fusión.

Para ejecutar este mandato, realice una copia de seguridad del servidor actual para los datos y la configuración. Cuando haya completado la copia de seguridad, instale el último release en el mismo servidor. A continuación, importe los datos y el archivo de configuración desde la CLI mediante el mandato import file. A continuación, después de importar los dos archivos de copia de seguridad, vuelva a ejecutar desde CLI el mandato restore db-from-prev-version. Esto restaura los archivos de copia de seguridad (datos y configuración) de la versión anterior en el servidor recién instalado.
Nota: Si está utilizando Guardium en un idioma distinto del inglés, el mandato de CLI restore establece algunas series, incluidas las cabeceras de informe, en inglés. Para ver estas series en un idioma que no sea el inglés, ejecute el mandato de CLI store language después de ejecutar el mandato de CLI restore.

El parámetro opcional "override" solo se aplica a una restauración de un dispositivo del Gestor central desde una copia de seguridad.

De forma predeterminada, cuando un usuario ejecuta el mandato "restore db-from-prev-version" desde un dispositivo del Gestor central, se conserva la información de configuración existente en este Gestor central que enlaza con las unidades gestionadas que gestiona.

Cuando el usuario añade "override" al mandato restore, se reemplaza la configuración de Gestor central/Unidades gestionadas existente por la configuración de Gestor central/Unidades gestionadas de los datos de copia de seguridad.

Sintaxis

restore db-from-prev-version [override]

Ejemplos

restore db-from-prev-version

restore db-from-prev-version override

Nota: Las unidades gestionadas y las asociaciones S-TAP en "Asociar S-TAP y unidades gestionadas" no se restauran cuando se utiliza este mandato de CLI. El usuario tiene que volver a definir las asociaciones.
Sintaxis

```
restore db-from-prev-version

Este procedimiento restaura y actualiza una copia de seguridad anterior en un sistema instalado recientemente. Si los archivos más
antiguos están actualmente ubicados en un sistema remoto, utilice el mandato de cli "import file" para transferirlos localmente
antes de ejecutar este procedimiento. Los archivos importados se guardan en el directorio /var/dump/. ¿Desea continuar (s/n)?
```

Nota:

Si responde sí a las preguntas siguientes durante la ejecución del mandato de CLI, restore db-from-prev-version, todos los informes y paneles no preconfigurados/personalizados se comprimen en un panel con el nombre Informes personalizados v.x.0.

Si responde no a las mismas preguntas, se restauran los mismos paneles como estaban en la versión anterior.

```
¿Desea actualizar el diseño del portal (la estructura de paneles y menús) al nuevo valor predeterminado de la versión 8 (las
instancias actuales de los informes personalizados se copiarán en el nuevo diseño, así como los cambios de parámetros en los
informes predefinidos) para el usuario admin? (s/n) n  ¿Desea actualizar el diseño del portal (la estructura de paneles y menús)
al nuevo valor predeterminado de la versión 8 (las instancias actuales de los informes personalizados se copiarán en el nuevo
diseño, así como los cambios de parámetros en los informes predefinidos) para todos los usuarios? (s/n)
```

restore keystore

Utilice este mandato únicamente siguiendo las instrucciones del servicio de soporte técnico.

Utilice este mandato para restaurar los certificados y las claves privadas que utiliza el entorno del contenedor de servlet web (Tomcat).

Sintaxis

restore keystore

restore pre-patch-backup

Utilice este mandato únicamente siguiendo las instrucciones del servicio de soporte técnico.

Utilice este mandato para restaurar pre-patch-backup cuando la base de datos del dispositivo esté activa o desactivada.

Sintaxis

```
restore pre-patchbackup Please enter the information to retrieve the file: Is the file in the local system? (y/n) n Start to
recover with the backup profile parameters. Please check the recovery status in the log
/var/log/guard/diag/depot/patch_installer.log ok ------------------------------------ If answer 'n', abort the operation. If
answer 'y', need to enter the file name.
```

restore system

Este tema se aplica a las operaciones de copia de seguridad y restauración de la base de datos interna de Guardium. Puede realizar una copia de seguridad o restauración únicamente de la información de configuración o de todo el sistema (datos más configuración del sistema, excepto los archivos de claves secretas compartidos, cuya copia de seguridad y recuperación se hace por separado, consulte los mandatos de copia de seguridad de archivos de clave de copia de seguridad y de restauración de archivos de clave del agregador). Estos mandatos detienen todos los motores de inspección y servicios web y los reinician cuando finaliza la operación.

Antes de restaurar un archivo, asegúrese de que el dispositivo tenga el secreto compartido del sistema para el sistema que ha creado el archivo, de lo contrario no podrá descifrar la información. Consulte la sección Acerca del secreto compartido del sistema en la guía de administración de Guardium.

Nota: La restauración del sistema se lleva a cabo en el mismo nivel de parche que la copia de seguridad del sistema.
Hay dos mandatos implicados en el proceso de restauración:

- import file, que devuelve un archivo de copia de seguridad archivado al sistema
- restore system, que restaura el sistema desde un archivo de seguridad que previamente ha devuelto una ejecución del mandato import file.

En todos los mandatos backup, import y restore, se le solicitará que proporcione una combinación de los elementos siguientes, en función de los sistemas de almacenamiento configurados y del tipo de operación de restauración. Responda a cada solicitud, según corresponda a su operación. La tabla siguiente describe la información que se le puede solicitar.

Nota:

Se guarda una copia de la transferencia de archivos SCP/FTP/TSM/Centera, independientemente de si se ha realizado correctamente o no la transferencia. Dado que algunos archivos pueden tardar horas en volver a generarse (por ejemplo, la copia de seguridad del sistema), es importante para el usuario tener preparada una copia disponible (sobretodo si falla la transferencia de archivos). Solo se retiene una copia de cada tipo de archivo (archivado/copia de seguridad del sistema/copia de seguridad de configuración/etc).

La copia de seguridad del sistema copia la licencia actual, la calibración y el número de orígenes de datos y, a continuación, realiza la copia de seguridad de los datos. La restauración del sistema restaura los datos y, a continuación, restaura la licencia, la calibración y el número de orígenes de datos. Esta secuencia se aplica a la restauración del sistema habitual. Si restaura desde un sistema anterior, es necesario volver a configurar la licencia, la calibración y el número de orígenes de datos.

Tabla 2. restore system

Elemento	Descripción
SCP, FTP, TSM, Centera, Snapshot	Seleccione el método que se ha de utilizar para transferir el archivo. Solo se muestran TSM y Centera si se han habilitado estos métodos de almacenamiento (consulte el mandato store storage-method)
Data o Configuration	Seleccione Configuración solo para las copias de seguridad de información de configuración y definiciones o seleccione Datos para la copia de seguridad de datos junto con la información de configuración.
restore from archive o restore from backup	Seleccione restore from archive para restaurar los datos archivos archivados o seleccione restore from backup para restaurar la información de configuración.
normal o upgrade	Si restaura desde la misma versión de software de Guardium, seleccione norma. Si restaura la información de configuración después de una actualización de software del dispositivo Guardium, seleccione upgrade.
host	El host remoto del archivo de copia de seguridad.
remote directory	El directorio del archivo de copia de seguridad. Para FTP, el directorio es relativo al directorio raíz de FTP para la cuenta de usuario FTP utilizada. Para SSH, la vía de acceso del directorio ha de estar completa. Para los servidores Windows SSH, utilice nombres de vías de acceso de estilo Unix con barras inclinadas, en lugar de barras invertidas como en Windows.
username	El nombre de la cuenta de usuario que se ha de utilizar para la operación (en operaciones de copia de seguridad, este usuario debe tener permiso de escritura/grabación para el directorio especificado). **Nota:** En Windows, se acepta un usuario de dominio con el formato dominio\usuario
password	La contraseña del nombre de usuario.
file name	El nombre de archivo del archivo de archivado o copia de seguridad. Consulte la sección Nombres de archivos de datos archivados. Puede seleccionar varios archivos utilizando el carácter comodín * en el nombre del archivo. Se permite el uso del carácter comodín * en los métodos de transferencia FTP, SCP y Snapshot. No se permite el uso del carácter comodín * en los métodos de transferencia TSM o Centera.
Centera server	Escriba el nombre del servidor Centera. Si utiliza archivos PEA, utilice el formato siguiente: <Nombre host/IP>? <nombre de archivo PEA completo>, por ejemplo: 128.221.200.56?/var/centera/us_profile_rwqe.pea.txt Tenga en cuenta el signo de interrogación ? entre las IP de servidor y el nombre de archivo Pea. Esta dirección IP y el archivo .PEA proceden de EMC Centera. El signo de interrogación es necesario cuando se configura la vía de acceso. El nombre de vía de acceso .../var/centera/... es importante, ya que puede fallar la copia de seguridad si no se sigue el nombre de vía de acceso. El archivo .PEA proporciona permisos y autenticación de nombre de usuario y contraseña por solicitud de copia de seguridad de Centera.
Centera clipID	En una operación de restauración de Centera, la dirección de contenido que devuelve la operación de copia de seguridad. Por ejemplo: 6M4B15U4JM4LBeDGKCPF9VQO3UA

Una vez se ha proporcionado toda la información necesaria para la operación de copia de seguridad o restauración, se muestra una serie de mensajes que informan acerca de los resultados de la operación. Por ejemplo, en una operación de restauración del sistema, los mensajes serán similares a los siguientes, en función del tipo de restauración y el método de almacenamiento utilizados:

```
gpg: Signature made Thu Feb 22 11:38:01 2009 EST using DSA key ID 2348FF9E gpg: Good signature from "Backup Signer
<support@guardium.com>" Proceeding to shutdown services Proceeding to startup services Safekeeping admin.xreg Safekeeping
client.xreg Safekeeping controllers.xreg Safekeeping controls.xreg Safekeeping guardium-portlets.xreg Safekeeping local-
portlets.xreg Safekeeping local-security.xreg Safekeeping local-skins.xreg Safekeeping media.xreg Safekeeping portlets.xreg
Safekeeping security.xreg Safekeeping skins.xreg guard_sniffer.pl -reorder Recovery procedure was successful. ok
```

set up help (disco secundario para copia de seguridad)

Instale un disco secundario o para copia de seguridad en dispositivos R610 R710. Insértelo en la ranura número 2 y continúe con la configuración de snapshotdisk para configurar la partición, formatear la unidad y montarla. Las dos opciones de CLI son setup help y setup snapshotdisk.

Sintaxis

setup [help | snapshotdisk | vmware_tools]

store language

Utilice este mandato de CLI para pasar de inglés de línea base y convertir la base de datos al idioma que desee. La instalación de Guardium siempre está en inglés. Un sistema Guardium se puede cambiar a japonés, chino (tradicional o simplificado), francés, español, alemán o portugués después de una instalación.

El mandato de CLI, store language, se considera una configuración del dispositivo y está diseñado para que se ejecute durante la configuración inicial del dispositivo.

Si se ejecuta este mandato de CLI, después del despliegue del dispositivo en un idioma específico, se puede cambiar la información ya capturada, almacenada, personalizada, archivada o exportada.

Nota: Después de cambiar de inglés a un idioma deseado, no puede revertir a inglés, utilizando este mandato de CLI. El sistema Guardium se debe volver a instalar en inglés.

Sintaxis

CLI > store language [Inglés | Japonés | Chino Simplificado | Chino Tradicional | Francés | Alemán | Español | Portugués]

Mandato show

show language

set up vmware tools

Utilice este mandato de CLI para instalar VMware que se ejecuta en la infraestructura ESX.

Sintaxis

setup vmware_tools [install | uninstall]

Paso 1: Abra el cliente/consola de la máquina virtual y seleccione la instancia de VM que contiene el dispositivo de IBM Guardium. Pulse la instancia en el motor derecho, el menú emergente seleccione Invitado => Instalar/actualizar herramientas de VMware. Esto permite que la instancia acceda a las herramientas VMware mediante un punto de montaje.

Paso 2: Ejecute el mandato de CLI (desde el cliente/consola de VM), setup vmware_tools install, para instalar las herramientas de VM.

Pánico después del reinicio del kernel Vmware

La máquina virtual VMware ESX 4.1 que se ejecutan en Guardium puede entrar en una situación de pánico después del reinicio del kernel.

Para corregir esta situación, VMware recomienda: Instalar la actualización 2 en ESX4.1 o Establecer la virtualización de CPU/MMU en Usar software solo para conjunto de instrucciones o Virtualización de MMU. Esta opción se encuentra bajo Valores/ Opciones/ CPU/MMU Usar software para conjunto de instrucciones y Virtualización de MMU.

Tema principal: Visión general de CLI

Mandatos de CLI del motor de inspección

Utilice estos mandatos de CLI para configurar el motor de inspección.

Un motor de inspección supervisa el tráfico entre un conjunto de uno o más servidores y un conjunto de uno o más clientes utilizando un protocolo de base de datos específico (por ejemplo, Oracle o Sybase). El motor de inspección extrae SQL de los paquetes de red, compila los árboles de análisis que identifican sentencias, solicitudes, mandatos, objetos y campos, y registra información detallada acerca de dicho tráfico en una base de datos interna.

add inspection-engines

Añade una configuración de motor de inspección al final de la lista de motores de inspección. Se describen los parámetros. Puede cambiar el orden de la lista de motores de inspección después de añadir uno nuevo, utilizando el mandato reorder inspection-engines. Cuando añade un motor de inspección éste no se inicia. Para iniciarlo, utilice el mandato start inspection-engines.

Sintaxis

add inspection-engines <name> <protocol>

<fromIP/mask> <port> <toIP/mask>

<exclude client list> <active on startup>

Parámetros

name - El nombre del nuevo motor de inspección. Debe ser exclusivo en la unidad.

protocol - El protocolo supervisado, que debe ser uno de los siguientes: Aster, Cassandra, CouchDB, DB2, DB2 Exit, exclude IE, FTP, GreenPlumDB, Hadoop, HIVE, HTTP, HUE, IBM ISERIES, IMPALA, Informix, iNFORMIX Exit, KERBEROS, Maria,DB, MongoDB, MS SQL, Mysql, Named Pipes, Netezza, Oracle, PostgreSQL, SAP Hana, Sybase, Teradata, WebHDFS or Windows File Share.

fromIP/mask - Una lista de clientes, identificados mediante direcciones IP y máscaras de subred. Separe cada dirección IP de su máscara con una barra inclinada y varias entradas con comas. Una dirección y máscara solo de ceros es un comodín. Si la opción de lista de clientes de exclusión (exclude client list) es Y, el motor de inspección supervisa el tráfico de todos los clientes, excepto los incluidos en esta lista. Si la opción de lista de clientes de exclusión (exclude client list) es N, el motor de inspección solo supervisa el tráfico de los clientes incluidos en esta lista.

port - El puerto o rango de puertos en los que se supervisará el tráfico entre los clientes y los servidores de base de datos especificados. Para especificar un rango, separe los dos números con un guion.

toIP/mask - La lista de servidores de base de datos, identificados mediante direcciones IP y máscaras de subred, cuyo tráfico se va a supervisar. Separe cada dirección IP de su máscara con una barra inclinada y varias entradas con comas. Una dirección y máscara solo de ceros es un comodín.

exclude client list - El valor es Y/N. El valor predeterminado es N. Si el valor es Y, el motor de inspección supervisa el tráfico de todos los clientes, excepto los incluidos en esta lista. El valor es N, el motor de inspección solo supervisa el tráfico de los clientes incluidos en esta lista.

active on startup - El valor es Y/N. El valor predeterminado es N. Si el valor es Y, se activa el motor de inspección cuando se arranca el sistema.

delete inspection-engines

Elimina un único motor de inspección identificado mediante su nombre. El nombre solo puede incluir letras, números y espacios en blanco. Si el nombre del motor de inspección contiene caracteres especiales, utilice la GUI del portal del administrador para eliminarlo.

Sintaxis

delete inspection-engines <name>

reorder inspection-engines

Especifica un nuevo orden para los motores de inspección, utilizando los valores de la lista que ha generado el mandato list inspection-engines.

Sintaxis

reorder inspection-engines <index>, <index>...

Ejemplo

Si los índices visualizados son 1, 2, 3 y 4, el mandato siguiente invertirá el orden de los motores:

reorder inspection-engines 4,3,2,1

restart inspection-core

Reinicia el núcleo de motores de inspección pero no los motores de inspección. Cuando se emite este mandato, se detiene la recopilación del tráfico de base de datos.

Sintaxis

restart inspection-core

Nota: Para reiniciar la recopilación de tráfico para uno o más motores de inspección específicos, siga este mandato con uno o más mandatos start inspection_engines. De forma alternativa, para reiniciar la recopilación del tráfico para todos los motores de inspección, utilice el mandato restart inspection-engines.

restart inspection-engines

Reinicia el núcleo de motores de inspección de base de datos y todos los motores de inspección. Mientras dura el proceso, se detiene la recopilación del tráfico de base de datos y solo se reinicia cuando se reinician las conexiones de base de datos.

Sintaxis

restart inspection-engines

show inspection-engines

Muestra la información acerca de la configuración del motor de inspección, de este modo:

all - Todos los motores de inspección.

configuration <index> - Solo los motores de inspección identificados en el índice especificado, que genera el mandato list inspection-engines.

type <db_type> - Muestra las configuraciones de un tipo de base de datos especificado, que debe ser uno de los tipos de protocolos supervisados soportados: Aster, Cassandra, CouchDB, DB2, DB2 Exit, exclude IE, FTP, GreenPlumDB, Hadoop, HIVE, HTTP, HUE, IBM ISERIES, IMPALA, Informix, iNFORMIX Exit, KERBEROS, Maria,DB, MongoDB, MS SQL, Mysql, Named Pipes, Netezza, Oracle, PostgreSQL, SAP Hana, Sybase, Teradata, WebHDFS or Windows File Share.

Sintaxis

show inspection-engines <all | configuration <index> | log sqlstrings | type <type> >

Nota: Utilice el mandato de CLI, show inspection-engines all, para visualizar los motores de inspección no de STAP, tal como los puertos SPAN. El mandato de CLI, list_inspection_engines, muestra los motores de inspección creados por STAP.

start inspection-core

Inicia el núcleo de motores de inspección.

Sintaxis

start inspection-core

start inspection-engines

Inicia uno o más motores de inspección, identificados mediante la lista que ha generado el mandato list inspection-engines.

Sintaxis

start inspection-engines <all | id>

start inspection-engines all

Inicia todos los motores de inspección.

Sintaxis

start inspection-engine all

start inspection-engines id

Uso: start inspection-engines id <n>, donde n es un id de sniffer numérico.

Sintaxis

start inspection-engines id <n>

stop inspection-engines id

Uso: stop inspection-engines id <n>, donde n es un id de sniffer numérico.

stop inspection-core

Detiene el núcleo de motores de inspección.

Sintaxis

stop inspection-core

stop inspection-engines

Detiene uno o más motores de inspección, identificados mediante la lista que ha generado el mandato list inspection-engines. También puede detener todos los motores de inspección.

Sintaxis

stop inspection-engine <all | id>

stop inspection-engines all

Detiene todos los motores de inspección.

Sintaxis

stop inspection-engines all

stop inspection-engines id

Detiene uno o más motores de inspección, identificados mediante la lista que ha generado el mandato list inspection-engines.

Sintaxis

stop inspection-engine <n>, donde <n> es el id de sniffer numérico

store ignored port list

Establece el conjunto completo de números de puertos que han de omitir todos los motores de inspección. La lista que especifique sustituirá por completo a la lista existente. Cada número está separado del siguiente por una coma, y no se permiten espacios en blanco ni otros caracteres de espacio en blanco en la lista. Utilice un guión para especificar un rango inclusivo de números.

Sintaxis

store ignored port list <n>

Ejemplo

store ignored port list 33,60-70

Mandato show

show ignored port list

Tema principal: Visión general de CLI

Mandatos de CLI del panel de control de investigación

Utilice estos mandatos de CLI para configurar el panel de control de investigación.

show solr connection_timeout

Utilice este mandato para mostrar el valor de connection_timeout actual.

```
show solr connection_timeout
```

show solr so_timeout

Utilice este mandato para mostrar el valor de so_timeout actual.

```
show solr so_timeout
```

show solr time_allowed

Utilice este mandato para mostrar el valor de time_allowed actual.

```
show solr time_allowed
```

store solr connection_timeout

Utilice este mandato para establecer el tiempo de espera de conexión. Si el panel de control de investigación no se puede conectar con el recopilador durante el periodo de tiempo de espera especificado, no se devuelve ningún resultado de dicho recopilador.

```
store solr connection_timeout [value]
```

Parámetro	Valor	Descripción
connection_timeout	entero	El tiempo de espera se expresa como un valor de `0` a `2147483647` milisegundos. El valor predeterminado es `100000` milisegundos.

store solr so_timeout

Utilice este mandato para establecer el tiempo de espera de socket.

```
store solr so_timeout [value]
```

Parámetro	Valor	Descripción
so_timeout	entero	El tiempo de espera se expresa como un valor de `0` a `2147483647` milisegundos. El valor predeterminado es `100000` milisegundos.

store solr time_allowed

Utilice este mandato para establecer el tiempo de espera de socket.

```
store solr time_allowed [value]
```

Parámetro	Valor	Descripción
time_allowed	entero	El tiempo de espera se expresa como un valor de `0` a `2147483647` milisegundos. El valor predeterminado es `90000` milisegundos. Nota: La búsqueda profunda utiliza 10x (diez veces) el valor de time_allowed.

Tema principal: Visión general de CLI

Mandatos de CLI de configuración de red

Utilice los mandatos de CLI de configuración de red para establecer dirección IP, manejar el acoplamiento/migración tras error, manejar las funciones secundarios y restablecer las redes.

Utilice los mandatos de CLI de configuración de red para:

- Identificar un conector en la parte posterior de la máquina (show network interface port)
- Restablecer la red después de instalar o mover una tarjeta de red (store network interface inventory)
- Establecer direcciones IP (store network interface ip, store network interface mask, store network resolver, store network routes defaultroute)
- Habilitar o inhabilitar la alta disponibilidad (store network interface high-availability)
- Configurar la tarjeta de red si el conmutador al que se conecta no realiza la negociación automática de los valores (store network interface auto-negotiation, store network interface speed, store network interface duplex)

restart network

Reinicia simplemente la configuración de la red. Por ejemplo, cambia la dirección IP y, a continuación, ejecuta este mandato de CLI.

Sintaxis

restart network

show network interface all

Este mandato muestra los valores de la interfaz de red utilizada para conectar el dispositivo Guardium a la LAN de escritorio. Se muestran la dirección IP, la máscara, el estado (habilitado o inhabilitado) y el estado de alta disponibilidad. Si está habilitada la función de alta disponibilidad IP, el sistema muestra dos interfaces (ETH0 y ETH3). De lo contrario, se muestra un ETH0.

Sintaxis

show network interface all

show network routes operational

Mostrar la configuración de direccionamiento de IP que se está utilizando.

Sintaxis

show network routes operational

Ejemplo

CLI> show net rout ope

Kernel IP routing table

Destination Gateway Genmask Flags Metric Ref Use Iface

192.168.3.0 0.0.0.0 255.255.255.0 U 0 0 0 nic1

169.254.0.0 0.0.0.0 255.255.0.0 U 0 0 0 nic2

0.0.0.0 192.168.3.1 0.0.0.0 UG 0 0 0 nic1

ok

CLI>

show network verify

Mostrar la configuración de direccionamiento de red actual.

Sintaxis

show network verify

```
CLI> show network verify

Current Network Configuration
-------------------------------------------------------------------------------
Hostname =
-------------------------------------------------------------------------------
Device     | Address         | Netmask         | Gateway         | Member of
-------------------------------------------------------------------------------
eth0       |
-------------------------------------------------------------------------------
Ethtool Options
-------------------------------------------------------------------------------
Device     | Options (speed,autoneg,duplex)
-------------------------------------------------------------------------------
eth0       |
-------------------------------------------------------------------------------
DNS Servers
-------------------------------------------------------------------------------
Index      | DNS Server
-------------------------------------------------------------------------------
1          |
2          |
-------------------------------------------------------------------------------
Static Routes
-------------------------------------------------------------------------------
Device     | Index      | Address         | Netmask         | Gateway
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Basic Network Settings Verified
```

store network interface auto-negotiation

Si está disponible la negociación automática en el conmutador al que está conectado un puerto Guardium, se utiliza la negociación automática y solo tendrá efecto la opción restart de este mandato. Utilice este mandato para habilitar, inhabilitar o reiniciar la negociación automática para la interfaz de red ethN. Utilice el mandato show network interface inventory para visualizar todos los nombres de puerto.

Sintaxis

store network interface auto-negotiation <ethN> <on | off | restart>

Mandato show

show network interface auto-negotiation

store network interface duplex

Utilice este mandato solo cuando la negociación automática no esté disponible en el conmutador al que está conectado el puerto Guardium. Este mandato configura la modalidad dúplex para el puerto ethn. Utilice el mandato show network interface inventory para visualizar todos los nombres de puerto.

Sintaxis

store network interface duplex <ethn> <half | full>

Mandato show

show network interface duplex <ethn>

store network interface high-availability

Habilita o inhabilita la agrupación de IP (conocida también como acoplamiento), que proporciona una función de migración tras error para la dirección IP primaria del sistema Guardium.

Los dos puertos utilizados (ETH0 y una segunda interfaz) deben estar conectados a la misma red. Se produce un ligero retardo, debido a que el conmutador debe volver a reconocer la configuración del puerto. El valor predeterminado es off.

El puerto utilizado para la dirección IP primaria siempre es ETH0. Cuando está habilitada la opción de alta disponibilidad, automáticamente se produce una migración tras error del sistema Guardium, según sea necesario, a la segunda interfaz especificada, lo que en la práctica significa que se transfiere la dirección IP primaria a la segunda interfaz.

Nota: La agrupación de IP y la interfaz secundaria no se pueden realizar al mismo tiempo.
Sintaxis:

```
store network interface high-availability [on <NIC> | off ]
```

No existe ningún mandato show network interface high-availability.

store network interface inventory

Restaura las direcciones MAC de la interfaz de red almacenadas en las tablas internas de Guardium. Este mandato solo se debe utilizar después de sustituir o mover una tarjeta de red.

Nota: El mandato store network interface inventory, detecta las tarjetas NIC incorporadas en el dispositivo Guardium y asigna estas tarjetas como eth0 y eth1. Este mandato solo se debe especificar si lo indica específicamente el servicio de soporte de Guardium, ya que puede cambiar el orden de las tarjetas NIC.

Sintaxis

```
CLI> > store network interface inventory
WARNING: Running this function will reorder your NICS and may make the machine unreachable.
WARNING: It is suggested to run this from the console or equivalent.
Are you SURE you want to continue? (y/n)
```

Utilice el mandato show para visualizar los nombres de puerto y las direcciones MAC de todas las interfaces de red instaladas.

Sintaxis

show network interface inventory

Ejemplo

CLI> show network interface inventory

Current network card configuration:

Device| Mac Address| Member of

eth0| 00:50:56:3b:c3:73|

eth1| 00:50:56:8a:0d:fa|

eth2| 00:50:56:8a:0d:fb|

eth3| 00:50:56:8a:00:c1|

Nota: “Member of” muestra los NIC del par de acoplamiento, si éste existe.

store network interface ip

Establece la dirección IP primaria para el dispositivo Guardium. Cuando cambia la dirección IP de la interfaz de red, es posible que también necesite cambiar su máscara de subred. Consulte store network interface mask. Consulte store network interface secondary para crear y gestionar una dirección IP secundaria. El acoplamiento y la migración tras error se gestionan desde el mandato de CLI, store network interface high-availability.

Sintaxis

store network interface ip <dirección ip>

Mandato show

show network interface ip

store network interface ip6

Establece la dirección IP V6 para el dispositivo Guardium. Cuando cambia la dirección IP de la interfaz de red, es posible que también necesite cambiar su máscara de subred. Consulte store network interface mask. Consulte store network interface secondary para crear y gestionar una dirección IP secundaria. El acoplamiento y la migración tras error se gestionan desde el mandato de CLI, store network interface high-availability.

Sintaxis

store network interface ip6 <dirección ip>

Mandato show

show network interface ip6

store network interface map

Correlaciona el puerto Ethernet identificado mediante ethn con la dirección MAC.

Sintaxis

store network interface map <ethn> <mac>

store network interface mask

Establece la máscara de subred para la dirección IP primaria. Cuando cambia la máscara de la interfaz de red, es posible que también necesite cambiar su dirección IP. Consulte store network interface ip. Tenga en cuenta que la máscara de subred de una dirección IP secundaria solo se puede asignar desde Configurar > Herramientas y vistas > Sistema.

Sintaxis

store network interface mask <máscara ip>

store network interface mtu

Utilice este mandato de CLI para establecer la MTU (Maximum Transfer Unit).

```
CLI> store network interface mtu
Uso: store network interface mtu <interface> <mtu>]
       donde <interface> es el nombre de interfaz,
       una de (eth0)
       y <mtu> es un número entre 1000 y 9000.
```

Mandato show

show network interface mtu

eth0 1500

show network interface port

Utilice este mandato para localizar un conector físico en la parte posterior del dispositivo. Después de utilizar el mandato *show network interface inventory* para visualizar todos los nombres de puerto, utilice este mandato para que parpadee el piloto del puerto físico especificado mediante una n (el dígito que sigue a eth - eth0, eth1, eth2, eth3, etc) 20 veces.

Sintaxis

show network interface port <n>

Ejemplo

CLI> show network interface port 1

Ahora el piloto naranja del puerto eth1 parpadeará 20 veces.

store network interface remap

Utilice este mandato de CLI para volver a correlacionar el NIC.

Sintaxis

store network interface remap

store network interface reset

Utilice este mandato de CLI para limpiar la configuración de red SO existente y volver a aplicar los valores de red de Guardium.

Sintaxis

```
CLI> store network interface reset
WARNING: This command will reset the network configuration to the stored Guardium network settings.
Are you SURE you want to continue? (y/n)
```

store network interface secondary

Utilice este mandato para configurar un puerto en el sistema Guardium como una interfaz de gestión secundaria con una dirección IP, máscara de red y pasarela diferentes de las de la interfaz primaria.

Nota: La agrupación de IP y la interfaz secundaria no se pueden realizar al mismo tiempo.
Sintaxis:

```
store network interface secondary [on <NIC> <ip> <mask> <gateway> | off ]
```

Mandato show

show network interface secondary

store network interface speed

Utilice este mandato solo cuando la negociación automática no esté disponible en el conmutador al que está conectado el puerto Guardium. Este mandato configura el valor de velocidad para el puerto ethn. Utilice el mandato show network interface inventory para visualizar todos los nombres de puertos.

Sintaxis

store network interface speed <ethn> <10 | 100 | 1000>

Mandato show

show network interface speed <ethn>

show network arp-table

Muestra la tabla ARP (Address Resolution Protocol) que es un valor del sistema operativo. Este mandato se proporciona únicamente para fines de servicio de soporte.

Sintaxis

show network arp-table

Ejemplo

CLI> sho net arp

IP address HW type Flags HW address Mask Device

192.168.3.1 0x1 0x2 00:0E:D7:98:07:7F * nic1

192.168.3.20 0x1 0x2 00:C0:9F:40:33:30 * nic1

ok

CLI>

show network macs

Muestra una lista de direcciones MAC, igual que el mandato show network interface inventory.

Sintaxis

show network macs

Ejemplo

Network card configuration:

Device| Mac Address| Member of

eth0| 00:50:56:3b:c3:73|

eth1| 00:50:56:8a:0d:fa|

eth2| 00:50:56:8a:0d:fb|

eth3| 00:50:56:8a:00:c1|

Nota: “Member of” muestra los NIC del par de acoplamiento, si éste existe.

ok

store network interface ip6

Uso: store network interface ip <ip>, donde IP es una dirección IP6 válida.

store network resolver

Establece la dirección IP del primero, segundo y tercer servidor DNS que ha de utilizar el dispositivo Guardium. Cada dirección de resolucionador debe ser exclusiva. Para eliminar un servidor DNS, especifique null en lugar de la dirección IP.

Sintaxis

store network resolver <1 | 2 | 3> <ip address | null>

Mandato show

show network resolver <1 | 2 | 3>

store network routes defaultroute

Establece la dirección IP del direccionador predeterminado en el valor especificado.

Sintaxis

store network routes defaultroute <ip address>

Mandatos show

show network routes defaultroute

store network routes static

Permitir que el usuario solo tenga una dirección IP por dispositivo (mediante eth0) y direccionar el tráfico a través de diferentes direccionadores mediante tablas de direccionamiento estático. Añadir línea a la tabla de direccionamiento estático.

Sintaxis

store network routes static

Mandato show

Lista las rutas estáticas actuales, con los ID - Dispositivo, Índice, Dirección, Máscara de red, Pasarela

show network routes static

Mandato delete

delete network routes static

store system domain

Establece el nombre de dominio del sistema en el valor especificado.

Sintaxis

store system domain <valor>

Mandato show

show system domain

store system hostname

Establece el nombre de host del sistema en el valor especificado.

Sintaxis

store system hostname <valor>

Mandato show

show system hostname

Tema principal: Visión general de CLI

Mandatos de CLI de soporte

Los siguientes mandatos de CLI solo se han de utilizar siguiendo las instrucciones del servicio de soporte técnico.

Estos mandatos ayudan al servicio de soporte técnico a analizar el estado de la máquina, resolver los problemas comunes y corregir algunos problemas comunes. No hay ninguna función que se realice de forma habitual con estos mandatos.

support clean audit_results

Un modo de depurar manualmente los resultados de la auditoría. Este mandato solo debe utilizarse cuando sea absolutamente necesario para manejar tareas de auditoría que generan un número elevado de registros y ocupan demasiado espacio de disco.

Antes de ejecutar este mandato, se recomienda consultar al servicio de soporte técnico.

Cuando se ejecuta este mandato, se muestra un mensaje de aviso y es necesario realizar una confirmación.

Este mandato lista los procesos de auditoría junto con información sobre las tareas.

Presenta el número de filas, ordenadas del conjunto de resultados mayor al conjunto de resultados más pequeño. El número de resultados del informe es mayor o igual al valor de entrada.

A continuación, una vez presentado el informe, el usuario puede selección un número de línea para depurar los resultados del proceso de auditoría correspondiente a dicho número de línea. Si se selecciona este número de línea, se suprimen los datos de auditoría para el nombre de proceso seleccionado.

Sintaxis

support clean audit_results <rows>

Parámetros de entrada

rows - un entero, número de filas que mostrar. Valor predeterminado: 10.

Nota: En un sistema con un gran número de tareas de auditoria, este mandato puede tardar algún tiempo en finalizar.

support clean log_files

Este mandato de CLI suprime el archivo especificado, después de que el usuario confirme la supresión. Si no encuentra el archivo, lista los archivos de más de 10MB en /var/log y el usuario suprime un archivo de gran tamaño de la lista. Se muestra un mensaje de aviso y se incluye un paso de confirmación.

Sintaxis

support clean log_file <filename> >> añadir nombre de archivo

support clean DAM_data

Un modo de depurar manualmente los resultados de la supervisión de la actividad de la base de datos. Este mandato solo debe utilizarse cuando sea absolutamente necesario.

Antes de ejecutar este mandato, se recomienda consultar al servicio de soporte técnico.

En el mandato se incluyen un mensaje de aviso y un paso de confirmación.

Sintaxis

support clean DAM_data <purge_type> <start_date> <end_date>

Parámetros de entrada

opciones de purge_type: agg, exceptions, full_details, msgs, constructs, access, policy_violations, parser_errors, flat_log

start_date: AAAA-mm-dd

end_date: AAAA-mm-dd

support clean centera_files

A los archivadores/copias de seguridad de Guardium, almacenados en Centera, Guardium les asigna una fecha de supresión, sin embargo, no existe un recurso que invoque posteriormente la supresión. Centera no tiene una GUI que permita el mantenimiento de sus propios archivos, se basa en las invocaciones de la API desde las aplicaciones de cliente.

Utilice el mandato de CLI, support clean centera_files, para suprimir los archivos marcados en Centera.

support clean InnoDB-dumps

Utilice este mandato de CLI para depurar tablas InnoDB

Este es un mandato protegido por contraseña (solo para el soporte técnico)

support clean hosts

USO: support clean hosts <dirección IP> <nombre de dominio completo>

support clean servlets

Suprime los archivos *jsp*.java and *jsp*.class y reinicia la GUI.

Utilice este mandato de CLI para suprimir los servlets Java™ generados y sus clases.

support execute

Este programa de utilidad esta diseñado para que el servicio de soporte avanzado de Guardium pueda ayudar en los diagnósticos remotos y proporcionar soporte cuando no se permita o esté disponible el acceso remoto directo.

Support Execute no sustituye a las conexiones remotas directas, pero permite que el servicio de soporte de Guardium tenga al menos algún nivel de acceso root seguro, sin el acceso directo.

Los mandatos que proporciona el servicio de soporte avanzado de Guardium pueden ser sentencias SQL, mandatos O/S, scripts Shell o scripts SQL. A continuación, se proporcionan al cliente junto con la clave segura para que puedan ejecutar el mandato mediante CLI. La clave segura está ligada al sistema en el que el servicio de soporte de Guardium trabaja con el cliente y no es válida para ningún otro sistema. El mandato solo se puede utilizar el número de veces que permita el servicio de soporte de Guardium y solo es válido durante siete días, a partir de la fecha acordada.

De forma predeterminada, la característica está inhabilitada. Puede habilitarla mediante un mandato de CLI en modalidad normal y en modalidad de recuperación:

support execute [enable | disable]

Para que el equipo del servicio de soporte avanzado de Guardium pueda generar una clave segura, se debe proporcionar la dirección MAC del sistema en cuestión para eth0. El siguiente es un ejemplo de las interfaces y las direcciones MAC:

Customer usage / Logged in as CLI

support execute <CMD String> <PMR #> <KEY>

main execute command provided by Guardium Advanced Support

support execute showlog [<Secure Key>|main|files]

Show usage logs

#'<Secure Key>' for full details of single entry

'main' to display the main execute log

'files' to display log directory list

support execute mac

Eth0 MAC address required by support to generate secure key

support execute info

Show eth0 MAC address, root passkey & other system information

support execute version

Display the "Support Execute" internal binary code version

support execute help

Help details and purpose of utility information

Ejemplo del mandato proporcionado por el servicio de soporte avanzado de Guardium:

support execute "select * from GDM_ACCESS%5CG" 11111,111,111 6254130c0f0c3c504b33687c57f41363e4c00

support reset-password accessmgr

Este mandato restaura la contraseña de la cuenta accessmgr.

Sintaxis

support reset-password accessmgr 10000000-99999999|random

Parámetros

Número de clave de 8 dígitos para generar la nueva contraseña. Conserve este número de clave para proporcionarlo al servicio de soporte técnico para que le entreguen la nueva contraseña de la cuenta accessmgr. La selección aleatoria genera un número aleatorio de 8 dígitos.

Nota: El sistema intenta enviar una notificación al correo electrónico de la cuenta accessmgr, si se ha configurado.

support reset-password root

Este mandato restaura la contraseña root en el dispositivo IBM® Guardium.

Sintaxis

support reset-password root 10000000-99999999|random

Parámetros

Número de clave de 8 dígitos para generar la nueva contraseña. Conserve este número de clave para proporcionarlo al servicio de soporte técnico. La selección aleatoria genera un número aleatorio de 8 dígitos.

Este mandato requiere que el usuario proporcione también una palabra clave secreta para poder cambiar la contraseña root. Póngase en contacto con el servicio de soporte técnico, si necesita cambiar la contraseña root.

Nota: No restablezca la contraseña root, a menos que lo requieran de forma absoluta las reglas empresariales.

support schedule find_crashed_tables

Utilice este mandato de CLI, support schedule find_crashed_tables [ON/OFF], para habilitar/inhabilitar el trabajo cron diario del script find_crashed_tables.sh.
USO: support schedule find_crash_tables on ALL|db
support schedule find_crash_tables off
Este mandato habilita o inhabilita la planificación diaria del script find_crashed_tables.
Nota: Preste una atención especial a la base de datos especificada. Se puede especificar "ALL" para procesar las cinco bases de datos válidas, si las tablas están bloqueadas, o simplemente una de las cinco bases de datos válidas "TURBINE", "GDMS", "CUSTOM", "DATAMART o "DIST_INT".

support show db-processlist

Este mandato lista todos los procesos de base de datos ordenados por tiempo de ejecución.

Sintaxis

support show db-processlist all

support show db-processlist locked

support show db-processlist running

support show db-process full

Parámetros:

support show db-processlist [ ]

Donde

running es la opción para ver todas las sentencias sql en ejecución

all es la opción para incluir los procesos en tiempo de inactividad

locked es para visualizar todos los procesos bloqueados y uno de los procesos más antiguos

full [opcional] muestra las consultas sql en formato expandido

support show db-struct-check

Este mandato muestra todas las diferencias de estructura encontradas durante el proceso de agregación.

Sintaxis

support show db-struct-check

support show db-top-tables

Este mandato lista las 20 tablas de base de datos más grandes, ordenadas por tamaño, y la lista de tablas ordenadas por espacio de tabla libre en porcentaje, para aquellas tablas que utilizan más del 80% del espacio libre. Permite filtrar por nombre de tabla. Todos los tamaños de tabla se muestran en Mbytes, el uso de espacio libre en porcentajes.

Sintaxis

support show db-top-tables all

support show db-top-tables like

Parámetros

support show db-top-tables all

lista las tablas de mayor tamaño del total de la BD clasificada

support show db-top-tables like

lista las tablas más grandes que coinciden con el criterio, donde puede haber cualquier parte del nombre de tabla

support show db-status

Este mandato muestra el uso de la base de datos.

Las selecciones son free, used, megabytes, percentage.

Sintaxis

support show db-status free %

support show db-status used %

support show db-status free m

support show db-status used m

support show hardware-info

Este mandato utiliza un script para recopilar información de hardware y colocar esta información recopilada en un directorio para su recuperación.

Después de ejecute este mandato de CLI, se muestra el mensaje siguiente:

Collected HW Info as /var/log/guard/Gather_hw_info-2012-06-25-17-43.tgz

A continuación, ejecute el mandato de CLI, fileserver, para recuperar este archivo .tar del servidor.

support show iptables

Este mandato muestra la salida del mandato iptables del sistema.

Sintaxis

support show iptables diff

support show iptables list

Parámetros

[diff | list] parámetro que controla la presentación de la salida de iptables, en lugar de mostrar solo diferencias/delta

[accept | full] parámetro que lista la salida aceptando filas y no listas filtradas

support show large_files

Este mandato lista todos los archivos con mayor número de MB y más antiguos en días de las carpetas /var /tmp /root.

Uso

support show large_files

Este mandato lista todos los archivos con mayor número de MB y más antiguos en días de las carpetas /var /tmp /root

Parámetros de entrada:

* size - entero > 10 (in MB)

* age - entero >= 0 (en días)

Sintaxis:

support show large_files <size> <age>

Parámetros

support show large_files

donde <size> es el tamaño mínimo de los archivos que se han de visualizar (predeterminado 100M)

donde <age> es el número de días desde la última modificación.

support show netstat

Este mandato muestra la salida del mandato netstat del sistema. Permite filtrar la salida por contenido utilizando el parámetro grep.

Sintaxis

support show netstat all

support show netstat grep

Parámetros

support show netstat grep

where es la serie alfanumérica que se ha de buscar

support show netstat all

support show port open

Este mandato es similar a utilizar telnet para detectar un puerto TCP abierto localmente o en un host remoto.

Si se puede conectar correctamente, verá un mensaje similar al siguiente: Connection to 127.0.0.1 8443 port [tcp/*] succeeded!

Si no se puede conectar, verá un mensaje similar al siguiente: connect to 127.0.0.1 port 1 (tcp) failed: Connection refused

Sintaxis: support show port open

Puerto IP - La IP debe ser una dirección IPv4 válida, tal como 127.0.0.1.

El puerto debe ser un entero con un valor de 1-65535.

support show top

Este mandato muestra la salida del mandato top del sistema, clasificado por cpu, memoria o tiempo de ejecución. Se puede configurar el número de iteraciones (predeterminado 1) y el número de filas visualizadas (predeterminado 10).

Sintaxis

support show top [cpu | memory | time]

Parámetros

support show top cpu

siendo N el número de iteraciones, en un rango 1 -10, y R el número de filas a visualizar - mín. 10

support show top memory

siendo N el número de iteraciones, en un rango 1 -10, y R el número de filas a visualizar - mín. 10

support show top time

siendo N el número de iteraciones, en un rango 1 -10, y R el número de filas a visualizar - mín. 10

support check tables [nombre BD] [nombre tabla}

Invoca el mandato mysqlcheck –c en las tablas (comprueba si hay errores en las tablas).

Sin parámetros, este mandato comprueba todas las tablas de la base de datos TURBINE con un tiempo de espera de 3 minutos para cada comprobación. Las comprobaciones se ejecutan en paralelo y el tiempo global varía. El mandato muestra el progreso en porcentajes. Si cualquier comprobación se ejecuta durante

más de 3 minutos, finaliza. Una vez finalizado el mandato, en la pantalla se muestran todas las tablas cuyas comprobaciones han finalizado debido a un tiempo de espera excedido. Los errores que se produzcan durante la operación del mandato se notifican en el archivo de registro /var/log/guard/<nombrebd>_check_tables/errors.<fecha>.log, donde <fecha> es la fecha actual y <nombrebd> el nombre de la base de datos.

Los errores encontrados en cada operación de comprobación de tabla se notifican en los archivos /var/log/guard/<nombrebd>_check_tables/check_table_child.<nombretabla>.<fecha>.log, donde <fecha> es la fecha actual, <nombrebd> es el nombre de la base de datos y <nombretabla> es el nombre de la tabla comprobada. No se crean archivos para las tablas cuyo estado sea correcto. Si nombrebd se especifica como el primer parámetro, el mandato comprueba todas las tablas de la BD especificada con el mismo tiempo de espera (3 minutos). Si no se especifican parámetros, comprueba todas las tablas de TURBINE.

Si se especifican nombrebd y nombretabla como los parámetros, el mandato comprueba la tabla especificada en la BD especificada, sin tiempo de espera, hasta que se completa la operación de comprobación. Esto permite una comprobación manual de las tablas cuya comprobación no ha finalizado en el periodo de 3 minutos. Puede utilizar máscaras en el parámetro nombretabla, utilizando el signo de porcentaje (%).

support shrink innodb-size

Utilice este mandato de CLI para reducir el tamaño del archivo ibdat1.

Realiza los pasos siguientes:

- vuelca todas las tablas InnoDB
- detiene mysql
- suprime los archivos ibdata1, ib_logfile0, ib_logfile1
- inicia mysql
- restaura las tablas volcadas

Este es un mandato protegido por contraseña (solo para el soporte técnico)

support show innodb-status

Utilice este mandato de CLI para resolver problemas de MySQL. Utilice este mandato de CLI para comprobar lo que sucede con las tablas MySQL en tiempo de ejecución. Utilice este mandato de CLI para determinar si los periodos de tiempo largos de la comprobación de las tablas MySQL son debidos a un bloqueo de registro o un bloqueo de tabla.

```
support show innodb-status
```

0 queries inside InnoDB, 0 queries in queue

0 read views open inside InnoDB

Main thread process no. 7959, id 139923805550336, state: sleeping Number of rows inserted 6894, updated 6934, deleted 93, read 24787 0.33 inserts/s, 0.00 updates/s, 0.00 deletes/s, 0.67 reads/s

---

END OF INNODB MONITOR OUTPUT

support analyze static-table

Utilice este mandato de CLI para analizar el contenido de las tablas estáticas ordenándolas por el grupo más grande por longitud de valor y la aparición del valor.

mandatos support must_gather

Hay algunos mandatos must_gather simples que puede ejecutar el usuario de CLI para generar información específica acerca del estado de cualquier sistema Guardium. Esta información se puede cargar desde el dispositivo y enviar al servicio de soporte técnico de Guardium siempre que se registra un PMR (Problem Management Record).

Para ejecutar estos mandatos, necesita tener instalado el parche must_gather adecuado.

Una vez instalado el parche correcto, el usuario de CLI puede ejecutar los mandatos must_gather en cualquier momento, del modo siguiente.

1. Abra una sesión Putty (o similar) en el sistema Guardium adecuado.
2. Inicie sesión como usuario de CLI.
3. En función del tipo de problema que tenga, pegue los mandatos must_gather relevantes en la solicitud de CLI. Es posible que se necesite más de un mandato must_gather para diagnosticar el problema.

   support must_gather system_db_info

   support must_gather purge_issues

   support must_gather audit_issues

   support must_gather agg_issues

   support must_gather cm_issues

   support must_gather alert_issues

   support must_gather patch_install_issues

La siguiente ejecución puede tardar algunos minutos en completarse.

support must_gather miss_dbuser_prog_issues

support must_gather sniffer_issues

En los mandatos siguientes, se le solicitará el periodo de tiempo en minutos que desea que se ejecute el depurador mientras reproduce el problema.

support must_gather backup_issues

support must_gather scheduler_issues

La salida se graba en el directorio must_gather con nombres de archivos similares a los de este ejemplo, must_gather/system_logs/.tgz

4. Envíe la salida resultante al servicio de soporte de IBM.

Si utiliza fileserver, puede cargar los archivos tgz y enviarlos al servicio de soporte.

Puede enviarlo por correo electrónico o subirlo a ECUREP utilizando, por ejemplo, una transferencia de datos estándar y especificando el número de PMR y el archivo que desea cargar.

Mandatos de diagnósticos de tráfico de Guardium for z/OS

support store zdiag on [N]

Donde N, opcional, es el número de minutos para la ejecución de los diagnósticos, entre 10 a 600, siendo el valor predeterminado 60

Activa los diagnósticos de tráfico de Guardium for z/OS. Esto incluye la recopilación de TCPDUMP y SLON. Las recopilaciones se detienen cuando los archivos correspondiente alcanzan un tamaño de 2 GB. Una vez completado, los archivos de resultados tcpdump.tar.gz y slon_all.tar.gz se pueden encontrar con el mandato fileserver. La partición /var debe tener al menos 15 GB de espacio libre.

support store zdiag off

Desactiva los diagnósticos de tráfico de Guardium for z/OS. Puede descargar los archivos de resultados tcpdump.tar.gz y slon_all.tar.gz utilizando el mandato de CLI fileserver.

support show zdiag

Muestra el estado de los diagnósticos de tráfico de Guardium for z/OS.

Mandatos de recopilación SLON

support store slon on [parámetro]

Activa el programa de utilidad SLON que captura paquetes obtenidos mediante sniffer para su depuración. Puede encontrar los archivos de resultados slon_packets.tar.gz, slon_messages.tar.gz o slon_all.tar.gz utilizando fileserver. La partición /var debe tener al menos 15 GB de espacio libre.

Donde el parámetro opcional es:

packets, volcar paquetes de analizador (predeterminado)

snifsql, registrar actividades SQL de sniffer y volcar paquetes de analizador

secparams, registrar información de parámetros seguros y volcar paquetes de analizador

sgate, registrar información de depuración de S-GATE y volcar paquetes de analizador

messages, volcar datos de mensajes tap

support store slon off [parámetro]

Desactiva el programa de utilidad SLON. Puede encontrar los archivos de resultados slon_packets.tar.gz, slon_messages.tar.gz o slon_all.tar.gz utilizando fileserver.

Donde el parámetro opcional es:

packets, detener volcado de paquetes, registrar parámetros seguros, información de depuración de S-GATE y actividades SQL de sniffer (predeterminado)

messages, detener volcado de datos de mensajes de tap

all, detener todas las actividades

support show slon

Muestra el estado del programa de utilidad SLON.

Mandato de recopilación TCPDUMP

support store snif_memory_max
Uso: support snif_memory_max <num>, donde num es un número | 33 | 50 | 75 |
Este mandato solo se aplica al sistema de 64 bits.
Mandato show
support show snif_memory_max

support store tcpdump on <type> <period> <loglimit> [interface] [IP] [port] [protocol]

support store tcpdump on <type> <period> <loglimit> [interface] [IP] [port] [protocol]

Activa el programa de utilidad TCPDUMP. Cuando finaliza el periodo, puede encontrar el archivo de resultados tcpdump.tar.gz utilizando fileserver. La partición /var debe tener al menos 15 GB de espacio libre.

Donde:

<type> - tipo de volcado, 'headers' (solo captura cabeceras) o 'raw' (captura paquetes completos)

<period> - periodo de volcado, NUMBER[SUFFIX], SUFFIX es opcional y puede ser 's' para segundos, 'm' para minutos (predeterminado)

<loglimit> - límite de volcado de archivo de registro, de 1 a 6 gigabytes

Argumentos de filtro opcionales:

[interface] - nombre de interfaz de red (predeterminado eth0)

[IP] - dirección IP

[port] - puerto

[protocol] - protocolo, 'tcp', 'udp', 'ip', 'ip6', 'arp', 'rarp', 'icmp' o

'icmp6'

Ejemplo

support store tcpdump on headers 10m 1

Este mandato ejecuta TCPDUMP, guarda las cabeceras de paquetes durante 10 minutos y el límite de tamaño de archivo de registro es de 1 GB.

support show tcpdump

Muestra el estado del programa de utilidad TCPDUMP.

support store tcpdump off

Desactiva el programa de utilidad TCPDUMP. Cuando finaliza, puede encontrar el archivo de resultados tcpdump.tar.gz utilizando fileserver.

support must_gather datamining_issues

Recopila la información de diagnóstico necesaria para las funciones de valores atípicos, búsqueda rápida y despensa de datos. La información incluye volcados de las tablas internas correspondientes, los registros necesarios, el estado de los procesos correspondientes y diagnósticos must_gather estándar (información general de la BD interna y del sistema).

support must_gather network_issues [--host=<HOST>], donde el parámetro opcional <HOST> es el nombre de host o la dirección IP.

El mandato recopila toda la información de red del dispositivo y sondea los hosts con los que interactúa Guardium utilizando ping, traceroute, sondeos de los puertos correspondientes y otras medidas. Si se especifica el parámetro opcional, solo sondea el host especificado (si se ha configurado Guardium para realizar cualquier actividad en este host).

store antlr3_max

Utilice este mandato de CLI para controlar el flujo de datos entre el analizador y el registrador. El mandato de CLI store antlr3_max es un parámetro avanzado para usuarios expertos y el servicio de soporte que ayuda a controlar el flujo de datos entre el componente Analizador y Registrador de Sniffer para Oracle, DB2, MySql y MSSql.

Este valor (cuyo valor predeterminado es 20.000) cambia el número de sentencias SQL analizadas simultáneamente que el registrador puede mantener en la cola.

Los problemas que puede ayudar a solucionar son la falta de memoria y el reinicio de Sniffer o si Sniffer no utiliza suficiente memoria.

Si observa que Sniffer se queda sin memoria suficiente y se reinicia, reducir la capacidad de contexto puede ayudar a aliviar este problema. De forma alternativa, si Sniffer no está utilizando la suficiente memoria del sistema disponible, aumentar la capacidad de contexto puede permitir que utilice más.

store active_parser_engine

Este mandato de CLI se utiliza para controlar qué motor del analizador debe utilizar Sniffer. Este mandato de CLI solo se aplica a los tipos de base de datos soportados por los analizadores ANTLR3 (Oracle, DB2, MS SQL, MySQL
USO: store active_parser_engine <num>
donde <num> es
1: ANTLR2 vuelve analizar los errores del analizador ANTLR3 (predeterminado)
2: Solo ANTLR2
3: Solo ANTLR3
Mandato show
show active_parser_engine

Tema principal: Visión general de CLI

Mandatos de CLI sistema

Utilice estos mandatos de CLI para configurar los valores del sistema.

store system apc

Utilice este mandato para configurar las opciones de apagado automático cuando está conectada una UPS. Tenga en cuenta que la UPS debe estar conectada a un conector USB (las conexiones serie para una UPS no están soportadas).

Establece el porcentaje de carga mínimo (0-100) antes de apagar, o el número de segundos que se debe ejecutar en alimentación de batería antes de apagar. Los valores predeterminados son 25 y cero, respectivamente.

También hay mandatos para iniciar y detener el proceso apc. De forma predeterminada, el proceso apc está inhabilitado.

Sintaxis

store system apc [battery-level <percent> | timeout <seconds>]

store system apc start

store system apc stop

Mandato show

show system apc [battery-level | timeout]

store system auditlog-passthrough

Utilice este mandato para habilitar o inhabilitar el paso a través de los datos del registro de auditoría desde el servicio auditd al syslog local. Dado que el registro de auditoría del sistema es detallado, la característica auditlog-passthrough se utiliza mejor junto con el registro remoto. Consulte Mandatos de CLI de configuración y control para obtener más información sobre el registro remoto.

De forma predeterminada, la característica auditlog-passthrough está inhabilitada.

Sintaxis: store system auditlog-passthrough [on | off]

Ejemplo:

```
> store sys aud on
Restarting auditd service to pick up the change.
Reloading configuration: [ OK ]
Auditd to syslog passthrough is enabled.
ok
```

Mandato show: show system auditlog-passthrough

store system banner

store system banner [message | clear]

Para crear un mensaje de banner (aviso sobre acceso no autorizado, mensaje de bienvenida, etc.) en el inicio de sesión de CLI, utilice el mandato de CLI, almacene el mensaje de banner [message | clear].

Sintaxis

store system banner clear - utilice este mandato CLI para eliminar un mensaje de banner existente.

store system banner message - utilice este mandato CLI para crear un mensaje de banner existente. Escriba el mensaje de banner y pulse Ctrl-D.

Mandato show

show system banner - utilice este mandato de CLI para ver un mensaje de banner existente.

store system clock datetime

Establece la fecha y hora del reloj del sistema en el valor especificado, donde **AAAA** es el año, **mm** es el mes, **dd** es el día, **hh** es la hora (en formato de 24 horas), **mm** son los minutos y **ss** son los segundos. Los segundos son necesarios, pero siempre se establecen en 00.

Sintaxis

store system clock datetime AAAA-mm-dd hh:mm:ss>

Mandato show

show system clock <all |datetime |timezone>

Ejemplo

store system clock datetime 2008-10-03 12:24:00

store system clock timezone

Lista el valor de huso horario permitido (opción de lista), o establece el huso horario de este sistema en el huso horario especificado. Utilice primero la opción de lista para visualizar todos los husos horarios y, a continuación, especifique el huso horario adecuado de la lista.

IBM® Guardium también registra el huso horario local en el seguimiento de auditoría estándar, para tratar los casos en los que los datos se utilizan en (o se agregan a) datos recopilados en otro husos horarios.

Nota: El valor de huso horario no se actualiza automáticamente durante el inicio del horario de verano. Para actualizar la máquina, el usuario debe restablecer el huso horario. Restablecer el huso horario significa establecer un nuevo huso horario, diferente del actual, y luego volver a establecerlo en el huso horario correcto. Restablecer simplemente el mismo huso horario no funciona y muestra el mensaje: No se ha cambiado el huso horario.

Sintaxis

store system clock timezone <list | timezone>

Mandato show

show system clock <all | timezone | datetime>

Ejemplo

En primer lugar, utilice el mandato con la opción **list** para mostrar todos los husos horarios. A continuación, escriba el mandato por segunda vez con el huso horario adecuado.

CLI> store system clock timezone list

Timezone: Description:

--- ---

Africa/Abidjan:

Africa/Accra:

Africa/Addis_Ababa:

...

...output deleted

...

CLI> store system clock timezone America/New_York

store system conntrack

Establece el estado actual del subsistema de seguimiento de conexiones del kernel de Linux. El estado puede ser ON|OFF.

Sintaxis

store system conntrack ON|OFF

Mandato show

show system conntrack

store system cpu profile

Permitir la configuración del escalado de CPU desde un mandato de CLI en hardware que admita el escalado de CPU.

Utilice este mandato de CLI para establecer una política de escalado de CPU que se ajuste a sus necesidades:

- conservative = menos uso de alimentación, escalado conservador
- balanced = uso medio de alimentación, escalado rápido en aumento
- performance = ejecuta la CPU a la velocidad máxima del reloj

El software de Guardium establece la política de escalado en Rendimiento después de la instalación.

Sintaxis

store system cpu profile [min|perf|max]

Mandato show

show system cpu profile

store system custom_db_size

Utilice este mandato de CLI para establecer el tamaño máximo de la tabla de base de datos personalizada (en MB). El valor predeterminado es 4000 MB.

Sintaxis

```
CLI> store system custom_db_max_size
USO: store system custom_db_max_size <N>
       donde N es un número mayor que 4000.
```

Mandato show

show system custom_db_size

store system domain

Establece el nombre de dominio del sistema en el valor especificado.

Sintaxis

store system domain <value>

Mandato show

show system domain

store system hostname

Establece el nombre de host del sistema en el valor especificado.

Sintaxis

store system hostname <value>

Mandato show

show system hostname

store system issue

store system issue [message | clear]

El mandato de CLI, store system issue message, recibe la entrada de la consola hasta Ctrl-d, y la graba en /etc/motd, después de eliminar de la entrada cualquier $,\, \ seguido de una sola letra y los caracteres `. Se trata de una forma de especificar mensajes que hacen que este sistema sea compatible con las políticas de seguridad de los clientes.

El mandato de CLI, store system issue clear, restaurará /etc/motd a la versión predeterminada.

La versión procede de /etc/guardium-release. Por ejemplo, SG70 -> 7.0, SG80 -> 8.0. Si no se encuentra SG en /etc/guard-release, la versión predeterminada es una serie vacía.

store system netfilter-buffer-size

Establecer el tamaño del almacenamiento intermedio netfilter.

Sintaxis

store system netfilter-buffer-size

Mandato show

Muestra el tamaño del almacenamiento intermedio netfilter de S-TAP. El valor predeterminado es 65536.

show system netfilter-buffer-size

show system ntp diagnostics

Utilice este mandato de CLI para ejecutar ntpq -p y ntptime y enviar directamente la salida a la pantalla. El sistema Guardium consulta ntpd desde localhost ´mediante udp.

Sintaxis

show system ntp diagnostics

Ejemplo

```
CLI> show system ntp diagnostics
Output from ntpq -p :
localhost.localdomain:
------------------------------------------------------------------------
Output from ntptime :
(Note that if you have just started the ntp server, it may report an 'ERROR' until it has synchronized.)
------------------------------------------------------------------
ntp_gettime() returns code 5 (ERROR)
  time d3443c21.47a46000  Thu, Apr 26 2012 17:26:57.279, (.279852),
  maximum error 16384000 us, estimated error 16384000 us
ntp_adjtime() returns code 5 (ERROR)
  modes 0x0 (),
  offset 0.000 us, frequency 0.000 ppm, interval 1 s,
  maximum error 16384000 us, estimated error 16384000 us,
  status 0x40 (UNSYNC),
  time constant 2, precision 1.000 us, tolerance 512 ppm,
```

store system ntp [all | server | state]

store system ntp server

Establece el **nombre de host** de un máximo de tres servidores NTP (Network Time Protocol). Tenga en cuenta que para habilitar el uso de un servidor NTP, debe utilizar el mandato **store system ntp state on**. Para definir un solo servidor NTP, escriba su nombre de host o dirección IP. Para definir varios servidores NTP, escriba el mandato sin argumentos y se le solicitará que proporcione los nombres de host de los servidores NTP.

Sintaxis

store system ntp server

USO: store system ntp server

Para cada servidor, especifique ip u hostname

Escriba un máximo de 3 servidores NTP para almacenar:

Mandato show

show system ntp <all |server>

Mandato delete

delete ntp-server

store system ntp state

Habilita o inhabilita el uso de un servidor NTP (Network Time Protocol) server.

Sintaxis

store system ntp state <on | off>

Mandato show

show system ntp <all |state>

store system patch install

Instala un solo parche o varios parches como un proceso en segundo plano. Las opciones **ftp** y **scp** copian un archivo de parche comprimido desde una ubicación de red al dispositivo IBM Guardium. Tenga en cuenta que un archivo de parche comprimido puede contener varios parches, pero solo se puede instalar un parche cada vez. Para instalar más de un parche, elija todos los parches que se han de instalar, separados por comas. Internamente, la CLI envía solicitudes para cada parche de la lista (en el orden especificado por el usuario) y el primer parche toma la hora de solicitud que ha especificado el usuario y cada uno de los parches posteriores tres minutos después del anterior. Además, la CLI comprueba si los parches especificados ya se han solicitado y no acepta solicitudes duplicadas.

La última opción (sys) se utiliza si se instala un segundo parche, o un parche siguiente, de un archivo comprimido que se ha copiado previamente en el dispositivo IBM Guardium utilizando este mandato.

Para ver una lista completa de los parches aplicados, consulte el informe Parches instalados en Gestionar > Informes > Gestión de instalación > Parches instalados, Gestionar > Mantenimiento > General > Parches instalados o Informes > Informes operativos de Guardium > Parches instalados.

En el mandato de CLI **install system patch install**, el usuario puede elegir varios parches de la lista.

Sintaxis

store system patch install <type> <date> <time>

<type> es el tipo de instalación, cd | ftp | scp | sys

<date> y <time> son la fecha y hora de la solicitud de instalación, con el formato AAAA-mm-dd para la fecha, y el formato hh:mm:ss para la hora.

Si no se especifica ninguna fecha y hora o si se especifica NOW, la hora de solicitud de la instalación es NOW.

Parámetros

Independientemente de la opción seleccionada, se le solicitará que seleccione un para aplicarlo:

Seleccione un parche para aplicarlo (1-n,q para salir):

cd- Para instalar un parche desde un CD, inserte el CD en la unidad de CD ROM de IBM Guardium antes de ejecutar este mandato. Se muestra una lista de los parches incluidos en el CD.

tp o **scp -** Para instalar un parche desde un archivo comprimido situado en cualquier ubicación de la red, utilice la opción **ftp** o **scp** y responda a las solicitudes que se muestran. Asegúrese de proporcionar el nombre completo de la vía de acceso para el parche, incluido el nombre de archivo:

Host desde el que importar el parche:

Usuario en nombre de host:

Vía de acceso completa al parche, incluido el nombre:

Contraseña:

En el mandato de CLI store system patch install scp, el usuario puede utilizar el carácter comodín * en el nombre de archivo de parche.

El archivo de parche comprimido se copia en el dispositivo IBM Guardium y se muestra una lista de los parches que incluye el archivo.

sys - Utilice esta opción para aplicar un segundo parche o un parche posterior desde un archivo de parches que se ha copiado previamente desde el dispositivo IBM Guardium mediante una ejecución anterior de store system patch.

El mandato store system patch install no suprime el archivo de parche del dispositivo IBM Guardium después de la instalación. Aunque realmente no es necesario eliminar el archivo de parche, dado que se pueden volver a instalar los mismos parches sobre los parches existentes y conservarlos puede ayudar solucionar diferentes problemas, el usuario puede eliminar los archivos de parche manualmente o utilizar el mandato de CLI diag. Tenga en cuenta que el mandato de CLI diag está restringido a determinados usuarios y roles.

Para suprimir una solicitud de instalación de parche, utilice el mandato de CLI delete scheduled-patch

store system public key reset

Después de generar las claves públicas SSH mediante los mandatos de CLI, show system public key tomcat o show system public key cli, con el mandato de CLI, store system public key reset, puede suprimir las claves SSH. Si las claves SSH no se han generado nunca, este mandato de CLI no hace nada. Este mandato solicita confirmación antes de la supresión.

Sintaxis

store system public key reset

store system remote-root-login

Habilitar/inhabilitar SSH (acceso root). Secure Shell o SSH es un protocolo de red que permite el intercambio de datos utilizando un canal seguro entre dos dispositivos en red.

Sintaxis

store system remote-root-login ON|OFF

Mandato show

show system remote-root-login

store system serialtty

En algunos entornos, TTY en serie no está disponible por lo que no se puede iniciar satisfactoriamente. Posiblemente, esto puede mostrarse en el registro del sistema y reenviarse a SIEM. Está habilitado de forma predeterminada para permitir la conectividad, pero puede inhabilitarse más adelante si se determina que las consolas en serie no están disponibles para el sistema.

Sintaxis

store system serialtty <on, off>

Mandato show

show system serialtty

Indica si las TTY de serie están habilitadas en el sistema.

Los informes son:

Las consolas TTY en serie están habilitadas en este sistema.

Las consolas TTY en serie están inhabilitadas en este sistema.

store system scheduler

La planificación se gestiona mediante un mecanismo de temporización en la aplicación IBM Guardium. Si interrumpe la función de temporización, se reiniciará después del intervalo de reinicio designado mediante el mandato de CLI.

Utilice store system scheduler restart_interval [5 to 1440 o -1] para reiniciar la función de temporización después de 5 minutos a 1440 minutos. El valor predeterminado es is -1, que indica que no está instalado el mecanismo de temporización de reinicio.

Utilice store system scheduler wait_for_shutdown [ON | OFF] para reiniciar el planificador una vez hayan finalizado todos los trabajos que se están ejecutando en este momento. Los parámetros son ON u OFF.

Sintaxis

store system scheduler restart_interval [5 - 1440 o -1]

store system scheduler wait_for_shutdown [ON | OFF]

Mandato show

show system scheduler

store system shared secret

Establece el valor del secreto compartido del sistema en el valor especificado. Esta clave debe ser la misma para un Gestor central y para todos los dispositivos que gestionará; o un Agregador y todos los dispositivos desde los que agrega datos. Cuando un dispositivo se registra para ser gestionado por un gestor central, ya no se utiliza el secreto compartido en dicha unidad. No puede anular el registro de una unidad en la Gestión central cambiando este valor.

La contraseña dinámico del usuario de SO del agregador

La contraseña del agregador será <la contraseña actual> concatenada con el secreto compartido, lo que significa: password=<contraseña actual><secreto compartido>

Los usuarios deberán asegurarse de que el secreto compartido de los recopiladores y el secreto compartido del agregador son exactamente iguales; de lo contrario, la transferencia SCP falla desde el recopilador al agregador. (Se trata de un requisito para unidades gestionadas y agregadores, recopiladores y agregadores, recopiladores y la pantalla de configuración de la exportación). El secreto compartido se puede establecer desde la CLI y desde el panel Sistema del separador Consola de administración.

Sintaxis

store system shared secret <key>

store system snif-alerts-facility

Este parámetro permite al usuario configurar el recurso para las alertas generadas por snif. Anteriormente las alertas generadas directamente por snif utilizaban el recurso de usuario, mientras que las alertas indirectas utilizaban el recurso de daemon (mediante el programa de utilidad guard_sender).

Sintaxis

store system snif-alerts-facility <facility>

USAGE: store snif-alerts-facility <facility>

El recurso es uno de los siguientes: daemon ftp local0 local1 local2 local3 local4 local5 local6 local7 lpr user

El valor predeterminado para el recurso es daemon.

Mandato show

show system snif-alerts-facility

store system snif-buffers-reclaim

Solo utilice este mandato de CLI cuando se lo indique el servicio técnico de IBM Guardium.

La nueva configuración entra en vigor cuando se ejecuta el mandato de CLI restart inspection-core.

Sintaxis

store system snif-buffers-reclaim [ON | OFF]

Mandato show

show system snif-buffers-reclaim

store system snif-thread-number

Utilice este mandato de CLI para especificar el número de hebras que se están ejecutando.

La nueva configuración entra en vigor cuando se ejecuta el mandato de CLI restart inspection-core.

Sintaxis

store system snif-thread-number [new | default]

Mandato show

show system snif-thread-number

Snif se está ejecutando con 6 hebras en un sistema de 32 bits

store system snmp contact

Almacena la dirección de correo electrónico para el contacto snmp (syscontact) para el dispositivo IBM Guardium. De forma predeterminada es info@guardium.com.

Sintaxis

store system snmp contact <email-address>

Mandato show

show system snmp contact

store system snmp location

Almacena la ubicación del sistema snmp (syslocation) para el dispositivo IBM Guardium. De forma predeterminada, es Unknown.

Sintaxis

store system snmp location <string>

Mandato show

show system snmp location

store system snmp query community

Almacena la comunidad de consulta del sistema snmp (syslocation) para el dispositivo IBM Guardium. De forma predeterminada, es guardiumsnmp.

Sintaxis

store system snmp query community <string>

Mandato show

show system snmp query community

Tema principal: Visión general de CLI

Mandatos de CLI de cuenta de usuario, contraseña y autenticación

Utilice estos mandatos de CLI para configurar las cuentas de usuario, las contraseñas y la autenticación.

Establecer la autenticación de guiuser

Cuando se inicia sesión mediante CLI, con una de las cuentas de CLI predeterminadas (guardcli1, ...guardcli5), es necesario ejecutar el mandato de CLI, set guiuser, para que funcionen todos los mandatos de GuardAPI. Esta autenticación es necesaria para impedir que los usuarios con roles limitados en la GUI accedan de forma no autorizada a los mandatos GuardAPI.

El uso de las cuentas guardcli1 ... guardcli5 requiere configurar una contraseña local. Utilice el mandato de CLI set guisuer para restablecer las cuentas guardcli1 ... guardcli5 y, a continuación, añada una contraseña local como se muestra en la sintaxis.

Algunos mandatos de CLI dependen del rol de guiuser. Por ejemplo, el rol de guiuser, que se marca cuando se crea un nuevo usuario desde la vista accessmgr, debe ser accessmgr para tener acceso a grdapi create_user, grdapi set_user_roles y grdapi update_user

Sintaxis

set guiuser <gui_user> password <contraseña>

Ejemplo

$ ssh guardcli1@a1.corp.com

IBM Security Guardium, Command Line Interface (CLI)

guardcli1@a1.corp.com's password:

Last login: Thu Nov 4 14:56:34 2012 from 123.a1.corp.com

==========

IBM Security Guardium

Unauthorized access is prohibited

==========

a1.corp.com> set guiuser johny_smith password 3wel9s887s

ok

a1.corp.com>

create_user

Ejemplos

>grdapi create_user firstName=john lastName=smith

password=pASSW0rd confirmPassword=pASSW0rd email=jsmith@us.ibm.com

userName=john disabled=0

ID=20000

```
>grdapi set_user_roles userName="john"
roles="dba,diag,cas,user"
```

ID=20000

Rol añadido (dba).

Se ha producido un fallo al añadir el rol (diag). Diag debe tener uno de estos roles: cli o admin.

Rol añadido (cas).

Rol añadido (user).

```
> grdapi set_user_roles userName="john"
roles="dba,diag,cas,user,cli"
```

ID=20000

Rol añadido (dba).

Rol añadido (diag).

Rol añadido (cas).

Rol añadido (user).

Rol añadido (cli).

```
> grdapi update_user userName="john"
email="john.smith@gmail.com"
```

ID=20000

> grdapi list_users

ID=0

####### User 3 #######

Username: accessmgr

First Name: accessmgr

Last Name: accessmgr

Email:

Disabled: false

####### User 1 #######

Username: admin

First Name: admin

Last Name: admin

Email:

Disabled: false

####### User 33 #######

Username: anon

First Name: anon

Last Name: anon

Email:

Disabled: false

####### User 20000 #######

Username: john

First Name: john

Last Name: smith

Email: john.smith@gmail.com

Disabled: false

####### User 2 #######

Username: bill

First Name: bill

Last Name: green

Email:

Disabled: true

set_user_roles

set_user_roles

Cada vez que se ejecuta un mandato set_user_roles, se restablecen los roles de un usuario. No ha de añadir a los roles. Debe restablecer.

Cuando crea un usuario utilizando GrdAPI, crea el usuario con el rol de usuario. Cuando establece el rol, tiene que especificar todos sus roles. Esto se lleva a cabo para permitir que se supriman los roles existentes y se añadan los roles nuevos.

Incluso en la GUI, se muestran todos los roles, de los puede seleccionar o deseleccionar un rol y cuando lo guarde, se guardará todo lo que ha seleccionado.

Lo que hace GrdAPI es asignar al usuario kevin solo el rol INV, donde cualquier usuario debe tener uno de estos roles: user, cli, admin o accessmgr

El modo correcto de invocar esta GrdAPI es:

```
grdapi set_user_roles userName="kevin"  roles="user,inv"
```

Ejemplo

> set guiuser accessmgr password ASDFasdf

ok

> grdapi create_user firstName=kevin

LastName=smith password=pASSW0rd confirmPassword=pASSW0rd

email=ksmith@company.com userName=kevin disabled=0

ID=20000

ok

```
> grdapi set_user_roles userName="kevin" roles="inv"
```

set_user_roles:

ERR=3700

El usuario debe tener uno de estos roles: user, cli, admin o accessmgr.

Error al ejecutar el mandato

ok

```
> grdapi set_user_roles userName="kevin"
```

```
roles="user,inv"
```

ID=20000

Rol añadido (user).

Se ha producido un fallo al añadir el rol (inv). Antes de asignar el rol inv, el apellido del usuario se debe establecer en el nombre de una de las tres bases de datos de investigación -

INV_1, INV_2 o INV_3 (distingue entre mayúsculas y minúsculas)

ok

```
> grdapi set_user_roles userName="kevin"
```

```
roles="dba,diag,cas,user"
```

ID=20000

Rol añadido (dba).

Se ha producido un fallo al añadir el rol (diag). Diag debe tener uno de estos roles: cli o admin.

Rol añadido (cas).

Rol añadido (user).

ok

>

show guiuser

Muestra el usuario (por rol) de la GUI.

Mandato show

show guiuser

Mandatos de control de contraseña

Utilice los siguientes mandatos para controlar las contraseñas de usuario, de este modo:

- store password disable - Establecer el número de días después del cual se inhabilita una cuenta inactiva.
- store password expiration - Establecer el número de días después del cual caduca la contraseña.
- store password validation - Habilitar o inhabilitar las reglas de validación de contraseña reforzadas.

Mandatos account lockout

Utilice los mandatos account lockout para inhabilitar una cuenta de usuario de Guardium después de varios intentos de inicio de sesión fallidos. Utilice estos mandatos para:

- Habilitar o inhabilitar la característica. Consulte store account lockout.
- Establecer el número máximo de errores de inicio de sesión permitidos en una cuenta durante un periodo de tiempo especificado. Consulte el mandato store account strike count y el mandato store account strike interval.
- Establecer el número máximo de errores permitidos en una cuenta durante la vida útil del dispositivo Guardium. Consulte el mandato store account strike max.
- Para desbloquear la cuenta del usuario admin si se bloquea consulte la descripción del mandato unlock admin.

Después de inhabilitar una cuenta de usuario de Guardium, la pueden habilitar desde el portal de Guardium únicamente los usuarios con el rol accessmgr o el usuario admin.

Ejemplo

Habilitar el bloqueo de cuentas, bloquear una cuenta después de 5 errores de inicio de sesión en un periodo de 10 minutos y establecer el número máximo de errores permitido en 999.

store account lockout on

store account strike count 5

store account strike interval 10

store account strike max 999

Nota:

Si la cuenta del usuario admin está bloqueada, utilice el mandato unlock admin para desbloquearla.

Cuando está habilitado el bloqueo de cuentas, si se establece strike count o strike max en cero NO se inhabilita este tipo de comprobación. Por el contrario, significa que después de un único error, se inhabilitará la cuenta.

store account lockout

Habilita (on) o inhabilita (off) la función de bloqueo de cuentas automático, que inhabilita una cuenta de usuario después de un número de errores de inicio de sesión especificado.

Sintaxis

store account lockout <on | off>

Mandato show

show account lockout

store account strike count

Establece el número de intentos de inicio de sesión anómalos (n) en el intervalo de strike configurado antes de inhabilitar la cuenta.

Sintaxis

store account strike count <n>

Mandato show

show account strike count

store account strike interval

Establece el número de segundos (n) durante el cual se debe producir el número de configurado de intentos de inicio de sesión a anómalos, para que se inhabilite la cuenta.

Sintaxis

store account strike interval <n>

Mandato show

show account strike interval

store account strike max

Establece el número máximo (n) de intentos de inicio de sesión anómalos permitidos para una cuenta durante la vida útil de servidor, antes de que se inhabilite la cuenta.

Sintaxis

store account strike max <n>

Mandato show

show account strike max

store password disable

Establece el número de días de inactividad, después del cual se inhabilitarán las cuentas. Si se establece en 0 (cero), no se inhabilitará ninguna cuenta debido a su inactividad. Durante la instalación, el valor predeterminado es cero. Debe reiniciar la GUI después de cambiar este valor (consulte restart gui).

Sintaxis

store password disable <días>

Mandato show

show password disable

store password expiration

Establece la antigüedad (en días) de caducidad de la contraseña de usuario. Si se establece en -1, la contraseña no caduca nunca. Para cualquier otro valor, se debe restaurar la contraseña la primera vez que se inicia sesión después de que haya caducado la contraseña actual. El valor predeterminado es 90. Debe reiniciar la GUI después de cambiar este valor.

Sintaxis

store password expiration <días>

Mandato show

show password expiration

store password validation

Activa o desactiva la validación de contraseña. El valor predeterminado es on. Cuando se ejecuta este mandato, se reinicia la GUI para aplicar este valor.

Cuando está habilitada la validación de contraseña, la contraseña debe tener ocho o más caracteres y debe incluir al menos un carácter alfabético en mayúsculas (A-Z), un carácter alfabético en minúsculas (a-z), un dígito (0-9) y un carácter especial de la tabla. Cuando se inhabilita (no se recomienda), se permite cualquier longitud o combinación de caracteres.

Sintaxis

store password validation <on | off>

Mandato show

show password validation

Tabla 1. Caracteres especiales para contraseñas Guardium

Carácter	Descripción
@	Signo de arroba
#	Signo de almohadilla
$	Signo de dólar
%	Signo de porcentaje
^	Acento circunflejo
&	Ampersand
.	Punto
;	Punto y coma
!	Signo de exclamación
-	Guión (menos)
+	Signo más
=	Signo de igual
_	Guión bajo (subrayado)

store user password

Utilice este mandato para restablecer la contraseña del usuario de cli. Para simplificar el proceso del servicio de soporte, le recomendamos que conserve la contraseña del usuario de cli que ha asignado inicialmente Guardium. No hay ningún modo de recuperar la contraseña de usuario de cli una vez establecida. Si pierde esta contraseña, póngase en contacto con el servicio de soporte de Guardium para restablecerla.

Sintaxis

store user password

Se le solicitará que especifique la contraseña actual y, a continuación, la nueva contraseña (dos veces). Ninguno de los valores de contraseña que especifique en el teclado se mostrarán en la pantalla.

Los requisitos para las contraseñas de usuario de cli difieren de los requisitos de las contraseñas de usuario. La contraseña de usuario de cli debe tener al menos seis caracteres y debe contener al menos uno de cada uno de los tipos de caracteres siguientes:

- Dígitos (0-9)
- Caracteres alfabéticos en minúsculas (a-z)
- Caracteres alfabéticos en mayúsculas (A-Z)

Cuando se ejecuta este mandato de CLI también se actualiza el registro de cambio de periodo de tiempo en el archivo de caducidad de contraseña.

unlock accessmgr

Utilice este mandato para habilitar la cuenta del usuario accessmgr de Guardium después de que se haya inhabilitado. Este mandato no restaura la contraseña de la cuenta del usuario accessmgr.

Nota: Solo los usuarios con el rol admin pueden ejecutar este mandato de CLI.

Sintaxis

unlock accessmgr

restart gui

unlock admin

Utilice este mandato para habilitar la cuenta del usuario admin de Guardium después de que se haya inhabilitado. Este mandato no restaura la contraseña de la cuenta del usuario admin.

Nota: Solo los usuarios con el rol admin pueden ejecutar este mandato de CLI.

Sintaxis

unlock admin

restart gui

Mandatos de autenticación

Los siguientes mandatos muestran o controlan el tipo de autenticación utilizado.

store auth

Utilice este mandato para restablecer en SQL_GUARD el tipo de autenticación utilizado para iniciar sesión en el dispositivo Guardium, por ejemplo, la autenticación de Guardium local, que es el valor predeterminado.

Se pueden configurar y habilitar métodos de autenticación opcionales, LDAP o Radius, por ejemplo, desde el portal del administrador pero no desde la CLI. Para obtener más información, consulte la sección Configurar la autenticación.

Sintaxis

store auth SQL_GUARD

Mandato show

show auth

Tema principal: Visión general de CLI

Referencia de GuardAPI

GuardAPI proporciona acceso a las funciones de Guardium desde la línea de mandatos.

Permite la automatización de tareas repetitivas, lo cual es especialmente importante en las implementaciones de gran tamaño. Utilizar estas funciones de GuardAPI permite realizar rápidamente operaciones como crear orígenes de datos, mantener jerarquías de usuarios o mantener las características de Guardium, tales como S-TAP, por mencionar algunas.

Para iniciar sesión en CLI correctamente para utilizar GuardAPI, es necesario iniciar sesión con una de las cinco cuentas de CLI (guardcli1,...,guardcli5) y un inicio de sesión adicional (utilizando el mandato 'set guiuser') con un usuario (username/guiuser de GUI) que ha creado el gestor de acceso y al que ha asignado el rol admin o cli. Para obtener más información, consulte la sección Establecer la autenticación de guiuser.

GuardAPI es un conjunto de mandatos de CLI que empiezan todos por la palabra grdapi.

- Para listar todos los mandatos GuardAPI disponibles, escriba el mandato grdapi sin argumentos o utilice el mandato 'grdrdapi commands' sin ningún argumento de búsqueda. Por ejemplo:

```
CLI> grdapi
o
CLI> grdapi commands
```

- Para ver los parámetros de un mandato concreto, escriba el mandato siguiente seguido de '--help=true'. Por ejemplo:

```
CLI> grdapi list_entry_location --help=true
ID=0
function parameters :
fileName
hostName - required
path - required
ok
```

- Para buscar mandatos de GuardAPI proporcionando una serie de búsqueda, utilice el mandato de CLI, grdapi commands <cadena-búsqueda>. Por ejemplo:

```
CLI> grdapi commands user
ID=0
Matching API Function list :
create_db_user_mapping
create_user_hierarchy
delete_allowed_db_by_user
delete_db_user_mapping
delete_user_hierarchy_by_entry_id
delete_user_hierarchy_by_user
execute_appUserTranslation
execute_ldap_user_import
list_allowed_db_by_user
list_db_user_mapping
list_user_hierarchy_by_parent_user
update_user_db
```

- Para visualizar una lista de valores para un parámetro, escriba el mandato seguido de '--get_param_values=<parámetro>;'. Por ejemplo:

```
CLI> grdapi create_group --get_param_values=appid
Value for parameter 'appid' of function 'create_group' must be one of:
Public
Audit Process Builder
Classifier
DB2 zOS Groups
Express Security
IMS zOS Groups
Policy Builder
Security Assessment Builder
ID=0
ok
```

Tabla 1. Las API que dan soporte a la estructura de mandatos – get_param_values

Función de API	Parámetro
create_datasource	application, type, severity, shared
create_group	appid, type

Distinción entre mayúsculas y minúsculas

Los componentes de palabra clave y valor de los parámetros distinguen entre mayúsculas y minúsculas.

Valores de parámetros con espacios

Si un valor de parámetro contiene uno o varios espacios, debe estar encerrado entre comillas dobles.

Por ejemplo:

```
grdapi create_datasource type ="MS SQL SERVER" ...
```

Valores nulos y series vacías

En general, cuando se invoca una función de GuardAPI y no se especifica para un parámetro que no es necesario o se establece como una serie vacía (""""), GuardAPI convierte dicho parámetro en un valor NULL cuando se invoca la función de GuardAPI. Esto significa que GuardAPI omite el parámetro como si no se hubiera especificado.

Por ejemplo, si desea borrar un grupo de una regla de política, establezca dicho grupo en un espacio vacío ("" "") y no en una serie vacía (""""). Utilizar una serie vacía (""""") indica a GuardAPI que ignore dicho grupo y no cambiará la selección de grupo.

Ejemplo para borrar un grupo de un valor de política

```
grdapi update_rule fromPolicy=V8 ruleDesc="LogFull Details" dbUserGroup=" " dbUser=" " objectGroup=" " commandsGroup=" "
```

Códigos de retorno

Independientemente del resultado del mandato GuardAPI, siempre se devuelve un código de retorno en la primera línea de salida, con el formato siguiente:

Tabla 2. Códigos de retorno

Código de retorno	Descripción
ID=identifier	Se ha realizado correctamente. El identificador es el ID del objeto en el que se ha realizado la operación. Por ejemplo, ele ID de un grupo que se acaba de definir.
ERR=error_code	Error. error_code identifica el error y se proporcionan una o varias líneas adicionales con una descripción del error. La sección Visión general incluye una tabla de errores comunes y la sección Códigos de error de GuardAPI incluye la lista completa de los códigos de error.

Por ejemplo, si se utiliza el mandato create_group para definir correctamente un grupo de objetos con el nombre agroup, se devuelve el ID de dicho grupo:

```
CLI> grdapi create_group desc=agroup type=objects appid=Public
ID=20001
ok
CLI>
```

Se puede utilizar dicho ID en el mandato list_group_by_id para visualizar la definición del grupo

```
CLI> grdapi list_group_by_id id=20001
ID=20001
Group GroupId=20001
Group GroupTypeId=3
Group ApplicationId=0
Group GroupDescription=agroup
Group GroupSubtype=null
Group CategoryName=null
Group ClassificationName=null
Group Timestamp=2008-05-10 07:34:11.0
Group type = OBJECTS
Application Type = Public
Touple Group
ok
```

Si el mandato no se ejecuta correctamente, se devuelve un código de error. Por ejemplo, si se vuelve a ejecutar el mandato list_group_by_id con un ID no válido, se recibe el mensaje siguiente:

```
a1.corp.com> grdapi list_group_by_id id=20123
ERR=140
Could not retrieve Group - check Id.
ok
```

Códigos de error comunes

Los códigos de error con un valor menor que 100 son condiciones de error comunes. Los códigos de error con un valor mayor que 100 se aplican a funciones específicas y se describen después de cada función.

Para ver una lista completa de los códigos de error de GuardAPI, escriba grdapi-errors en el indicador de mandatos de CLI.

Tabla 3. Códigos de error comunes

Error	Descripción
0	Faltan parámetros o se han producido errores desconocidos, como excepciones imprevistas.
1	Se produjo una excepción, póngase en contacto con el soporte de Guardium
2	No se pudo recuperar la función seleccionada - compruebe el nombre de la función. Para listar todas las llamadas de función ejecute los mandatos de CLI grdapi o grdapi, sin argumentos. Para buscar mediante una serie de búsqueda un nombre de función, utilice el mandato de CLI, grdapi commands <cadena-búsqueda>
3	Demasiados argumentos. Para obtener la lista de parámetros de esta función llame a la función con --help=true
4	Faltan argumentos necesarios. Para obtener la lista de parámetros de esta función llame a la función con --help=true

Error	Descripción
5	No se pudo descifrar parámetro, compruebe si se ha cifrado con el secreto compartido correcto.
6	El formato del parámetro es incorrecto, especifique un nombre de función seguido de una lista de parámetros utilizando el formato <nombre=valor>.
7	Valor de parámetro erróneo para el tipo de parámetro.
8	Nombre de parámetro erróneo, tenga en cuenta que los parámetros son sensibles a las mayúsculas y minúsculas.
9	El usuario no tiene suficientes privilegios para la función de API solicitada
10	El cifrado de parámetros no está habilitado, no se ha establecido el secreto compartido.
11	Se produjo un fallo al enviar una solicitud de llamada de API a targetHost
12	Error al validar el parámetro
13	El host de destino debe ser la dirección ip del gestor central
14	Este gestor no gestiona este host de destino
15	El host de destino no está en línea
16	No se puede especificar el host de destino en una unida autónoma
17	El usuario no tiene permiso para trabajar con el objeto especificado
18	No se puede especificar un host de destino
19	Faltan las comillas de cierre
20	El usuario no está autorizado a ejecutar mandatos grdapi
21	--username y --source-host son palabras reservadas de grdapi que no se pueden pasar en la línea de mandatos.
22	Un parámetro no se puede especificar más de una vez, compruebe la línea de mandatos para ver si hay parámetros duplicados.
23	El valor no está en la lista de constantes.
24	El valor cifrado no es válido.
25	El formato del parámetro no es válido - los parámetros se deben especificar como <nombre=valor>, no se permiten espacios.

Registro de actividad de GuardAPI

El registro de actividad de Guardium registra todos los mandatos grdapi que se ejecutan en el sistema. Para ver los mandatos desde el portal del administrador, vaya al informe Seguimiento de auditoría de actividad de usuario en el separador Supervisar de Guardium.

Toda la actividad de grdapi se atribuirá al usuario de cli. Pulse dos veces la fila de dicho informe y seleccione el informe Actividad detallada de usuarios de Guardium. Se listará cada mandato entrada, junto con cualquier cambio realizado. Asimismo, se lista la dirección IP desde la que se ha emitido el mandato.

Parámetro cifrado

GuardAPI está pensado para ser invocado con scripts, que pueden contener información confidencial, tal como contraseñas para orígenes de datos. Para asegurarse de que la información confidencial esté cifrada en todo momento, el mandato grdapi permite pasar un parámetro cifrado a una función de API. Este cifrado se lleva a cabo utilizando el secreto compartido del sistema, establecido por el administrador, y que puede ser compartido por muchos sistemas, y por todas las unidades de una gestión central o de clúster de agregación, si se habilitan los scripts con parámetros cifrados para que se ejecuten en las máquinas que tienen el mismo secreto compartido.

Nota: Si se ejecuta una llamada a la API con un parámetro cifrado en un sistema que no tiene establecido el secreto compartido, se genera el mensaje de error

```
El cifrado de parámetros no está habilitado, no se ha establecido el secreto compartido
```

En el caso de los scripts de la API Guard generados mediante la GUI, si se requiere cifrado, éste se lleva a cabo utilizando el secreto compartido del sistema en el que se genera el script.

El parámetro opcional encryptedParam está disponible en cada llamada a grdapi. Este parámetro se puede utilizar para pasar un valor cifrado para otro parámetro.

El procedimiento para el cifrado manual es el siguiente:

1. Utilizar la API de cifrado de parámetros

   La API encrypt_value acepta un valor para cifrarlo y el secreto compartido (clave) del sistema de destino, a continuación, emite el valor cifrado. Si la clave no es el secreto compartido del sistema, muestra un aviso.

```
a1.corp.com> grdapi encrypt_value --help=true
ID=0
function parameters :
key - required
valueToEncrypt - required
api_target_host
ok
```

Tabla 4. Parámetro cifrado

Parámetro	Descripción
key	El secreto compartido del sistema de destino
valueToEncrypt	El valor que se ha de cifrar
api_target_host	Solo en una configuración de gestión central, permite al usuario especificar un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
a1.corp.com> grdapi encrypt_value valueToEncrypt="some value" key=guard
ID=0
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.7 (GNU/Linux)
jA0EAgMCTEIUShudn0tgyTB9GL7wR79UL9X9DCAa6RkUQRbegG52olA4gwOzmpHF
0qEhsd6Uz7l8rUsheUyX9v4=
=c1Cq
-----END PGP MESSAGE-----
```

2. Copie el contenido generado e inclúyalo en el script cli.

```
example of cli.gsh  code :
set guiuser johny_smith password 3wel9s887s
 grdapi create_datasource type=oracle name=myOra host=somehost application=AuditTask owner=admin user=sa serviceName=ora
encryptedParam=password
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.7 (GNU/Linux)
jA0EAgMCTEIUShudn0tgyTB9GL7wR79UL9X9DCAa6RkUQRbegG52olA4gwOzmpHF
0qEhsd6Uz7l8rUsheUyX9v4=
=c1Cq
-----END PGP MESSAGE-----
```

3. Ejecute el script para invocar GrdApi:

```
user> ssh cli@a1.corp.comuser> ssh cli@a1.corp.com
```

Precaución en la gestión central

Si utiliza GuardAPI en un entorno de gestión central, asegúrese de que comprende qué componentes se han definido en el Gestor central y qué componente se han definido en las unidades gestionadas. Para obtener más información sobre este tema, consulte Gestor central.

Visualizar atributos para determinados usuarios en el Creador de consultas

El usuario admin puede ver todos los atributos de consulta en el Creador de consultas y los usuarios que no son admin pueden ver los atributos en el Creador de consultas, excepto los que están diseñados solo para admin (por ejemplo, los ID).

Hay algunas entidades (tal como FULL SQL) que incluyen un gran número de atributos.

De forma predeterminada, se muestran todos los atributos para todos los usuarios (admin y no admin).

Se han añadido dos mandatos GuardAPI para visualizar o no visualizar determinados atributos para determinados usuarios.

Estos mandatos GuardAPI habilitarán o inhabilitarán SOLO grupos específicos de atributos en SQL completo: VSAM, ISAM, MApReduce, APEX, Hive y BigInsight.

Hay dos nuevas GuardAPI: grdapi enable_special_attributes y grdapi disable_special_attributes

Ambas solo reciben un parámetro: attributesGroup.

Los valores válidos de este parámetro son: VSAM, IMS, MapReduce, APEX, Hive, BI (BigInsights), IMS/VSAM, DB2 i, F5 (No distingue entre mayúsculas y minúsculas).

Cada Grdapi habilitará o inhabilitará todos los atributos correspondientes al grupo, por ejemplo, VSAM habilitará o inhabilitará los atributos siguientes:

- Registros VSAM
- Registros VSAM suprimidos
- Registros VSAM insertados
- Registros VSAM recuperados
- Registros VSAM actualizados
- ID de grupo de usuarios VSAM

Hive habilitará o inhabilitará los atributos siguientes:

- Mandato Hive
- Base de datos Hive
- Error de Hive
- SQL analizado por Hive
- Nombre de tabla Hive
- Usuario Hive

Nota: Los atributos se seguirán mostrando si el usuario tiene el rol admin. La habilitación o inhabilitación de estos atributos SOLO se aplica a los usuarios no admin (sin el rol admin).
Nota: No se ha de reiniciar la GUI para activar el cambio. Con esta excepción: Si se ha creado un informe con los atributos de grupo F5 y se ha añadido a Mis nuevos informes, aunque se hayan habilitado los atributos, el usuario no admin no tiene el privilegio para ver el informe. La GUI debe reiniciarse para ver los campos del informe.

- Funciones de archivado y restauración de GuardAPI
- Funciones de asesoramiento de GuardAPI
  Utilice estos mandatos de CLI para añadir, suprimir y actualizar las funciones de asesoramiento.
- Funciones de descubrimiento automático de GuardAPI
  Utilice estos mandatos de CLI para crear, modificar, listar y ejecutar funciones de descubrimiento automático.
- Funciones de entrada de catálogo de GuardAPI
  Utilice estos mandatos de GuardAPI para crear, listar, suprimir y actualizar funciones de entrada de catálogo.
- Funciones de clasificación de GuardAPI
  Utilice los siguientes mandatos GuardAPI para la configuración de política de clasificación, para la automatización de pruebas y para scripts de preparación de datos de requisito previo.
- Funciones de orígenes de datos de GuardAPI Cloud

- Funciones de usuario de base de datos de GuardAPI
  Utilice estos mandatos de GuardAPI para mantener la correlación de los usuarios de la base de datos, la exploración no de credenciales y establecer el nivel de depuración.
- Funciones de orígenes de datos de GuardAPI
  Utilice estos mandatos GuardAPI para crear, listar, suprimir y actualizar funciones de origen de datos.
- Funciones de referencia de orígenes de datos de GuardAPI
  Utilice estos mandatos GuardAPI para crear, listar, suprimir y actualizar funciones de referencia de orígenes de datos.
- Funciones de seguridad de usuario de datos de GuardAPI
  Utilice estos mandatos de GuardAPI para crear, listar, suprimir y actualizar funciones de seguridad de usuario de datos.
- Funciones de equilibrio de carga de empresa de GuardAPI
  Utilice estos mandatos de GuardAPI para ver y establecer los parámetros de equilibrio de carga, ver la correlación de la carga actual y gestionar las asociaciones de S-TAP y los grupos de unidades gestionados.
- Funciones de optimización de titularidades de GuardAPI
  Utilice estos mandatos de GuardAPI para habilitar y configurar los informes y orígenes de datos de optimización de titularidades.
- Funciones de canal de información externo de GuardAPI
  Utilice estas funciones GuardAPI para crear correlaciones para canales de información externos.
- Funciones de FAM (File Activity Monitor) de GuardAPI
  Utilice los siguientes mandatos de GuardAPI para habilitar e inhabilitar la actividad del supervisor de actividad de archivos, configurar la actividad del panel de investigación de archivos, la planificación de las extracciones de titularidad y obtener información acerca del supervisor de actividad de archivos.
- Funciones GIM de GuardAPI
  Utilice estos mandatos de CLI para listar, actualizar, asignar, eliminar y cancelar funciones GIM.
- Funciones de grupo de GuardAPI
  Utilice estos mandatos GuardAPI para crear, listar, suprimir y actualizar funciones de grupos de orígenes de datos.
- Generación de entrada de GuardAPI
  La generación de entrada de GuardAPI permite al usuario tomar la salida de un informe de Guardium y pasarla como entrada a otra entidad de Guardium. Lo permite a los usuarios utilizar llamadas preparadas para invocar las funciones de API.
- Funciones del panel de control de investigación de GuardAPI
  Utilice estos mandatos de GuardAPI para habilitar, inhabilitar o configurar parámetros y características del panel de control de investigación.
- Funciones de auditoría nativas de GuardAPI
  Utilice estos mandatos GuardAPI para habilitar, inhabilitar, la auditoría de base de datos (auditoría nativa) en la nube, para añadir y eliminar objetos de la auditoría nativa y para obtener objetos de configuración, recopiladores y objetos.
- Funciones de detección de valores atípicos de GuardAPI
  Utilice los mandatos GuardAPI siguientes para habilitar, inhabilitar y configurar la función de detección de valores atípicos.
- Funciones de control de procesos de GuardAPI
  Utilice estos mandatos GuardAPI para ejecutar, copiar, cargar, listar y suprimir las funciones de control de procesos.
- Funciones de reescritura de consultas de GuardAPI
  Automatice la realización o creación de pruebas o definiciones para determinadas consultas complejas que no se pueden realizar desde la interfaz de usuario utilizando las API de Guardium en la interfaz de línea de mandatos.
- Funciones de rol de GuardAPI
  Utilice estos mandatos de GuardAPI para otorgar, listar y revocar funciones de roles.
- Funciones de GuardAPI S-TAP
  Utilice estos mandatos de CLI para crear, listar, suprimir, reiniciar y establecer funciones de S-TAP.
- Funciones de detección de amenazas de GuardAPI

Tema principal: CLI y API

Funciones de archivado y restauración de GuardAPI

list_expiration_dates_for_restored_days

Listar las fechas de caducidad de todos los días restaurados.

Tabla 1. list_expiration_dates_for_restored_days

Parámetro	Descripción
newExpDate	Necesario. La nueva fecha de caducidad del día de restauración.
restoredDay	Necesario. Identifica el día de restauración de los datos.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

grdapi list_expiration_dates_for_restored_days

get_expiration_date_for_restored_day

Obtener la fecha de caducidad asociada a un día restaurado determinado.

Tabla 2. get_expiration_date_for_restored_day

Parámetro	Descripción
newExpDate	Necesario. La nueva fecha de caducidad del día de restauración.
restoredDay	Necesario. Identifica el día de restauración de los datos.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

```
grdapi get_expiration_date_for_restored_day restoredDay=restoredDay
```

donde restoredDay puede tener el formato de un día real `aaaa-mm-dd hh:mi:ss` o de un día relativo, tal como `NOW -10 day`.

set_expiration_date_for_restored_day

Establecer la fecha de caducidad asociada a un día restaurado determinado.

Tabla 3. set_expiration_date_for_restored_day

Parámetro	Descripción
newExpDate	Necesario. La nueva fecha de caducidad del día de restauración.
restoredDay	Necesario. Identifica el día de restauración de los datos.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

```
grdapi set_expiration_date_for_restored_day newExpDate=newExpDate restoredDay=restoredDay
```

donde newExpDate y restoredDay pueden tener el formato de un día real `aaaa-mm-dd hh:mi:ss` o un día relativo, tal como `NOW -10 day`.

set_import

Iniciar o detener la importación de datos de agregación.

Tabla 4. set_import

Parámetro	Descripción
state	Necesario. START o STOP
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi set_import [START]
```

configure_export

Configurar la exportación de datos de agregación.

Tabla 5. configure_export

Parámetro	Descripción
aggHost	Necesario. Serie. Nombre de host del agregador.
aggSecHost	Serie
exportOlderThan	Necesario. Entero. Detalles de los datos que se han de exportar por periodo de tiempo.
exportValues	Necesario. Entero. 0 o 1
ignoreOlderThan	Necesario. Entero. Detalles de los datos que se han de omitir por periodo de tiempo.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi configure_export [aggHost] [aggSecHost] [exportOlderThan] [exportValues] [ignoreOlderThan]
```

configure_archive

Configurar el archivado de datos de agregación.

Tabla 6. configure_archive

Parámetro	Descripción
accessKey	Serie. Clave se secreto compartido del agregador.
archiveOlderThan	Necesario. Entero. Detalles de los datos que se han de archivar por periodo de tiempo.
archiveValues	Necesario. Entero. 0 o 1
bucketName	Serie
destHost	Serie. Nombre del host del destino de archivado.
ignoreOlderThan	Necesario. Entero. Detalles de los datos que se han de omitir por periodo de tiempo.
passwd	Serie. Contraseña.
passwdRetype	Serie. Volver a escribir la contraseña
port	Entero. Número de puerto
protocol	Necesario. Serie. SCP, FTP o AMAZON
retention	Entero. El periodo de tiempo de retención.
secretKey	Serie
targetDir	Serie
userName	Serie. Nombre de usuario.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi configure_archive [accessKey] [archiveOlderThan] [archiveValues][bucketName][destHost][ignoreOlderThan][passwd]
[passwdRetype] [port] [protocol] [retention] [secretKey] [targetDir] [userName]
```

Tema principal: Referencia de GuardAPI

Funciones de asesoramiento de GuardAPI

Utilice estos mandatos de CLI para añadir, suprimir y actualizar las funciones de asesoramiento.

Utilice los mandatos de CLI siguientes para:

- Añadir, suprimir, actualizar la definición de asesoramiento de seguridad.
- Añadir, suprimir un origen de datos de un asesoramiento de seguridad existente.
- Añadir, suprimir pruebas de un asesoramiento de seguridad existente.

create_assessment

Utilice este mandato de GuardAPI para añadir un asesoramiento de seguridad.

Tabla 1. create_assessment

Parámetro	Validación
assessmentDescription	Necesario. Texto sin formato. Exclusivo. Debe asegurarse de que no exista un asesoramiento anterior con la misma descripción. Si existe uno, se muestra un ERROR.
fromDate	La fecha válida o la fecha relativa no son obligatorias. El valor predeterminado es NOW -1 DAY
toDate	La fecha válida o la fecha relativa no son obligatorias. El valor predeterminado es NOW
FilterClientIP	Dirección IP válida. No es obligatorio. El valor predeterminado es nulo.
FilterServerIP	Dirección IP válida. No es obligatorio. El valor predeterminado es nulo.

Acción: Si todos los parámetros se han validado, se crea un nuevo registro en la tabla SECURITY_ASSESSMENT (para MODIFIED_FLAG, dejar el valor predeterminado de 0)

Ejemplo

```
grdapi create_assessment assessmentDescription=Assess1
```

add_assessment_datasource

Utilice este mandato de GuardAPI para añadir un origen de datos a un asesoramiento de seguridad.

Tabla 2. add_assessment_datasource

Parámetro	Validación
assessmentDescription	Necesario. Texto sin formato. Exclusivo. Debe asegurarse de que no exista un asesoramiento anterior con la misma descripción. Si existe uno, se muestra un ERROR.
datasourceName	Necesario. Texto sin formato. Debe ser el nombre de un origen de datos existente, si no existe dicho origen de datos, se genera un ERROR

Acción: Si se validan todos los parámetros, se añade un registro a: ASSESSMENT_DATASOURCE utilizando ASSESSMENT ID y DATASOURCE ID para el asesoramiento y el origen de datos con los nombres proporcionados.

Ejemplo

```
grdapi add_assessment_datasource assessmentDescription=Assess1 datasourceName=DS1
```

add_assessment_test

Utilice este mandato de GuardAPI para añadir una prueba a un asesoramiento de seguridad existente.

Tabla 3. add_assessment_test

Parámetro	Validación
assessmentDescription	Necesario. Texto sin formato. Exclusivo. Debe asegurarse de que no exista un asesoramiento anterior con la misma descripción, si existe se genera un ERROR.
testDescription	Necesario. Texto sin formato: Debe coincidir con TEST_DESC de una prueba existente en AVAILABLE_TEST, si no está presente dicha prueba, se genera un ERROR.
severity	Se valida con la tabla SEVERITY_DESC (utilizando DESCRIPTION). No es obligatorio. El valor predeterminado es INFO.
thresholdValue	Si thresholdValue obligatorio de available_test = 0, IGNORAR este parámetro. De lo contrario, si valor (THRESHOLD) obligatorio de available_test = 1, el parámetro debe ser un entero. Si no se proporciona el parámetro, utilice DEFAULT_THRESHOLD_VALUE de AVAILABLE_TEST.

Parámetro	Validación
exceptionsGroup	Comprobar el valor de CAN_HAVE_EXCEPTIONS_GROUP en AVAILABLE_TEST. El parámetro NO es obligatorio. Si el valor es 0, entonces (el grupo de excepciones no está soportado para esta prueba): Si se proporciona el parámetro, entonces ERROR (no se puede proporcionar el grupo de excepciones para esta prueba). Si NO se proporciona el parámetro, entonces utilizar -1 para rellenar. De lo contrario, (el grupo de excepciones no está soportado para esta prueba): Si NO se proporciona el parámetro, entonces utilizar -1 para rellenar. Si se proporciona el parámetro, validar el grupo y utilizar el ID de grupo. Validar la selección de grupo desde GROUP_DESC, donde GROUP_DESCRIPTION = la descripción proporcionada, y comprobar si existe el registro y el GROUP_TYPE_ID Si se muestra el ERROR de que dicho grupo no existe, entonces no existe el grupo de excepciones. Si existe dicho grupo y GROUP_TYPE_ID != 55, entonces se muestra el ERROR: El grupo de excepciones debe ser del tipo “Excepciones VA". Si está presente el grupo y el tipo = 55, utilizar el GROUP_ID.

Validación adicional: Comprobar si ya existe un registro en ASSESSMENT_TEST para ASSESSMENT_ID y TEST_ID, si existe dicho registro se genera el ERROR: Esta prueba ya está presente en el asesoramiento y no se puede volver a añadir.

Acción: Si se validan todos los parámetros, entonces añadir un registro a ASSESSMENT_TEST (tenga en cuenta que se debe rellenar SEVERITY con DESCRIPTION)

Ejemplo

```
grdapi add_assessment_test  assessmentDescription=Assess1 testDescription="The first test"
```

delete_assessment

Utilice este mandato de GuardAPI para suprimir un asesoramiento de seguridad.

Tabla 4. delete_assessment

Parámetro	Validación
assessmentDescription	Necesario. Texto sin formato. Exclusivo. Debe asegurarse de que no exista un asesoramiento anterior con la misma descripción, si existe se genera un ERROR.

Validación adicional: Debe asegurarse de que no hay resultados para el asesoramiento que se ha de suprimir realizando lo siguiente:

Seleccionar recuento (*) desde ASSESSSMENT_RESULT_HEADER, donde ASSESSMENT_ID = TheIdToRemve

Si la selección devuelve > 0, entonces no eliminar, se genera un ERROR

Acción: Si se valida el parámetro, (identifica el registro de asesoramiento de seguridad y no hay resultados para el asesoramiento), suprimir los registros SECURITY_ASSESSMENT, los registros THE ASSESSMENT_TEST y los registros ASSESSMENT_DATASOURCE (utilizando ASSESSMENT_ID en las tres supresiones)

Ejemplo

```
grdapi delete_asssessment assessmentDescription=Assess1
```

delete_assessment_datasource

Utilice este mandato de GuardAPI para suprimir un origen de datos de un asesoramiento de seguridad.

Tabla 5. delete_assessment_datasource

Parámetro	Validación
assessmentDescription	Necesario. Texto sin formato. Exclusivo. Debe asegurarse de que no exista un asesoramiento anterior con la misma descripción. Si existe uno, se muestra un ERROR.
datasourceName	Necesario. Texto sin formato. Debe ser el nombre de un origen de datos existente, si no existe dicho origen de datos, se genera un ERROR

Acción: Si se validan todos los parámetros, comprobar si existe un registro en ASSESSMENT_DATASOURCE para el asesoramiento y el origen de datos proporcionados. Si no existe dicho registro, se genera un error, de lo contrario se suprime le registro.

Ejemplo

```
grdapi delete_asssessment_datasource assessmentDescription=Assess1 datasourceName=DS1
```

delete_assessment_test

Utilice este mandato de GuardAPI para suprimir una prueba de un asesoramiento de seguridad existente.

Tabla 6. delete_assessment_test

Parámetro	Validación
assessmentDescription	Necesario. Texto sin formato. Exclusivo. Debe asegurarse de que no exista un asesoramiento anterior con la misma descripción, si existe se genera un ERROR.

Parámetro	Validación
testDescription	Texto sin formato: Debe coincidir con TEST_DESC de una prueba existente en AVAILABLE_TEST, si no está presente dicha prueba, se genera un ERROR.

Validación adicional: Comprobar si ya existe un registro en ASSESSMENT_TEST para ASSESSMENT_ID y TEST_ID, si no existe dicho registro se genera el ERROR: Esta prueba no está presente en el asesoramiento.

Acción: Si se validan todos los parámetros, suprimir el registro de ASSESSMENT_TEST.

Ejemplo

```
grdapi delete_asssessment_test assessmentDescription=Assess1
```

list_assessments

Utilice este mandato de GuardAPI para listar los asesoramientos de seguridad.

Tabla 7. list_assessments

Parámetro	Validación
assessmentDescription	Necesario. Texto sin formato. Exclusivo. Debe asegurarse de que no exista un asesoramiento anterior con la misma descripción, si existe se genera un ERROR.

Ejemplo

```
grdapi list_assessments
```

list_assessment_tests

Utilice este mandato de GuardAPI para mostrar la lista de pruebas para el asesoramiento de seguridad.

La salida de list_available_tests tiene el formato siguiente: TEST=[<descripción de prueba>], DS_TYPE=[<tipo de origen de datos>] (los valores se encierran entre corchetes)

La salida de list_assessment_tests tiene el formato siguiente: TEST_DESC=[<descripción de prueba disponible>], DS_TYPE=[<tipo de origen de datos>]

Los parámetros del mandato de API list_assessment_tests no son obligatorios y soportan el filtrado.

Tabla 8. list_assessment_tests

Parámetro	Validación
assessmentDescription	Esta API: • Validará que la descripción sea UNA descripción de asesoramiento válida y recuperará el ID de asesoramiento. (Si no existe ningún asesoramiento, se genera un error) • Mostrará la lista de pruebas para el asesoramiento (y el tipo de origen de datos). Seleccionará AVAILABLE_TEST.TEST_DESC, DATASOURCE_TYPE.NAME desde ASSESSMENT_TEST, DATASOURCE_TYPE, AVAILABLE_TEST, SECURITY_ASSESSMENT, donde AVAILABLE_TEST.DATASOURCE_TYPE_ID = DATASOURCE_TYPE.DATASOURCE_TYPE_ID y ASSESSMENT_TEST.ASSESSMENT_ID = SECURITY_ASSESSMENT.ASSESSMENT_ID y SECURITY_ASSESSMENT.ASSESSMENT_DESC es igual que “Su Parám”

Ejemplo

```
grdapi list_assessment_tests
```

update_assessment

Utilice este mandato de GuardAPI para actualizar el registro del asesoramiento de seguridad.

Tabla 9. update_assessment

Parámetro	Validación
assessmentDescription	Debe coincidir con un registro existente en SECURITY_ASSESSMENT
newAssessmentDescription	Texto sin formato. Si está vacía, significa que no se actualiza la descripción, se utiliza el valor del parámetro anterior. De lo contrario, un valor exclusivo debe garantizar que no existe ningún asesoramiento con la misma descripción, si existe se genera un ERROR.
fromDate	Fecha válida o fecha relativa
toDate	Fecha válida o fecha relativa
filterContentIP	Dirección IP válida
filterServerIP	Dirección IP válida

Acción: Si se validan todos los parámetros (y se ha identificado un registro SECURITY_ASSESSMENT con la descripción suministrada, se actualiza el registro con los valores proporcionados)

Ejemplo

```
grdapi update_assessment assessmentDescription=Assess1 filterClientIP=192.168.1.1.
```

Tema principal: Referencia de GuardAPI

Funciones de descubrimiento automático de GuardAPI

Utilice estos mandatos de CLI para crear, modificar, listar y ejecutar funciones de descubrimiento automático.

add_autodetect_task

Este mandato añade una tarea al proceso especificado.

Tabla 1. add_autodetect_task

Parámetro	Descripción
process_name	Necesario. Nombre del proceso
hosts_list	Necesario. Listas de hosts. Es una lista separada por espacios de direcciones IP o rangos de IP y comodines, tal como 192.168.0.1 192.168.1.*
ports_list	Necesario. Lista de puertos. Es una lista separada por comas de puertos o rangos de puertos, tal como 22,23,1400-1600
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi add_autodetect_task process_name=myProcess hosts_list="192.168.1.1 192.168.1.3" ports_list="22,23"
```

create_autodetect_process

Este mandato crea un proceso de detección automática.

Tabla 2. create_autodetect_process

Parámetro	Descripción
check_ICMP_echo	Necesario. Parámetro PE para nmap (*). Los valores son 'true' o 'false'
host_timeout	Necesario. Parámetro que se ha de correlacionar (*). Valor de tiempo de espera.
process_name	Necesario. Nombre del proceso
run_probe_after_scan	Necesario. Los valores son 'true' o 'false'.
use_dns	Necesario. Parámetro para nmap[1]. Los valores son 'R' o 'true' para siempre, 'n' o 'false' para nunca.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Nota: * Únicamente se puede acceder a las opciones nmap desde la API y no desde la GUI. Para obtener detalles acerca de los parámetros nmap y su impacto en el rendimiento de la exploración, consulte man nmap.

Ejemplo

```
grdapi create_autodetect_process process_name=myProcess
```

modify_autodetect_process

Este mandato modifica un proceso de detección automática.

Tabla 3. modify_autodetect_process

Parámetro	Descripción
check_ICMP_echo	Necesario. Parámetro PE para nmap (*). Los valores son 'true' o 'false'
host_timeout	Necesario. Parámetro que se ha de correlacionar (*). Valor de tiempo de espera.
process_name	Necesario. Nombre del proceso

Parámetro	Descripción
run_probe_after_scan	Necesario. Los valores son 'true' o 'false'.
use_dns	Necesario. Parámetro para nmap[1]. Los valores son 'R' o 'true' para siempre, 'n' o 'false' para nunca.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Nota: * Únicamente se puede acceder a las opciones nmap desde la API y no desde la GUI. Para obtener detalles acerca de los parámetros nmap y su impacto en el rendimiento de la exploración, consulte man nmap.

Ejemplo

```
grdapi modify_autodetect_process process_name=myProcess
```

delete_autodetect_scans_for_process

Este mandato elimina todas las tareas de un proceso, pero no se puede ejecutar si un proceso está en ejecución, se ha planificado o tiene resultados.

Tabla 4. delete_autodetect_scans_for_process

Parámetro	Descripción
process_name	Necesario. Nombre del proceso
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi delete_autodetect_scans_for_process process_name=myProcess
```

list_autodetect_processes

Este mandato lista todos los procesos.

Tabla 5. list_autodetect_processes

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi list_autodetect_processes
```

list_autodetect_tasks_for_process

Este mandato lista todas las tareas de un proceso especificado.

Tabla 6. list_autodetect_tasks_for_process

Parámetro	Descripción

Parámetro	Descripción
process_name	Necesario. Nombre del proceso
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi list_autodetect_tasks_for_process process_name=myProcess
```

execute_autodetect_process

Este mandato ejecuta el proceso especificado, pero no se puede ejecutar si no hay ninguna tarea definida para el proceso o si el proceso se está ejecutando actualmente.

Tabla 7. execute_autodetect_process

Parámetro	Descripción
process_name	Necesario. Nombre del proceso
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi execute_autodetect_process process_name=myProcess
```

show_autodetect_process_status

Este mandato muestra un resumen del progreso y el estado del proceso.

Tabla 8. show_autodetect_process_status

Parámetro	Descripción
process_name	Necesario. Nombre del proceso
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi show_autodetect_process_status process_name=myProcess
```

stop_autodetect_process

Este mandato detiene la ejecución de un proceso específico.

Tabla 9. stop_autodetect_process

Parámetro	Descripción
process_name	Necesario. Nombre del proceso

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi stop_autodetect_process process_name=myProcess
```

Tema principal: Referencia de GuardAPI

Funciones de entrada de catálogo de GuardAPI

Utilice estos mandatos de GuardAPI para crear, listar, suprimir y actualizar funciones de entrada de catálogo.

create_entry_location

Añada una nueva entrada de archivado en la tabla de la ubicación del catálogo interno.

Tabla 1. create_entry_location

Parámetro	Descripción
entryType	Serie necesaria. Debe ser uno de los siguientes: • CollectorDataArchive • AggDataArchive • AggResultArchive
processDesc	Serie. Se utiliza y solo es necesaria cuando entryType es AggResultArchive.
fileName	Serie necesaria. Identifica el archivo.
hostName	Serie necesaria. Identifica el host.
path	Serie necesaria. Para FTP: Especifique el directorio relativo al directorio de inicio de la cuenta de FTP. Para SCP: Especifique el directorio como una vía de acceso absoluta.
user	Serie necesaria. Cuenta de usuario para acceder al host.
password	Serie necesaria. La contraseña del usuario.
retention	Entero opcional. El número de días que esta entrada se va a conservar en el catálogo (el valor predeterminado es 365).
storageSystem	Serie necesaria. Debe ser uno de los siguientes: EMC CENTERA, FTP, SCP, TSM.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi  create_entry_location entryType=CollectorDataArchive  fileName=733392-a1.corp.com-w20071223.133546-d2007-12-27.dbdump.enc
password=somePassword user=someUser path=/var/dump/ hostName=192.168.1.241  storageSystem=scp
```

list_entry_location

Lista una ubicación de archivado si se ha especificado un fileName, o lista varias ubicaciones de archivado cuando se omite fileName.

Tabla 2. list_entry_location

Parámetro	Descripción

Parámetro	Descripción
fileName	Serie opcional. Identifica la ubicación de un solo archivo que se ha de listar. Si se omite, se listarán todas las ubicaciones de archivo de hostName y path.
hostName	Serie necesaria. Identifica el host.
path	Serie necesaria. Para FTP: Especifique el directorio relativo al directorio de inicio de la cuenta de FTP. Para SCP: Especifique el directorio como una vía de acceso absoluta.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi list_entry_location   path=/mnt/nfs/ogazit/archive_results/ hostName=192.168.1.33
```

delete_entry_location

Actualiza una ubicación de archivado si se ha especificado un fileName o elimina varias ubicaciones de archivado cuando se omite fileName.

Tabla 3. delete_entry_location

Parámetro	Descripción
fileName	Serie opcional. Identifica la ubicación de un solo archivo que se ha de eliminar. Si se omite, se eliminan todas las ubicaciones de archivo de hostName y path.
hostName	Serie necesaria. Identifica el host.
path	Serie necesaria. Para FTP: Especifique el directorio relativo al directorio de inicio de la cuenta de FTP. Para SCP: Especifique el directorio como una vía de acceso absoluta.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi delete_entry_location  path=/var/dump/mojgan hostName=192.168.1.18
```

update_entry_location

Actualiza una ubicación de archivado si se ha especificado un fileName o actualiza varias ubicaciones de archivado cuando se omite fileName.

Tabla 4. update_entry_location

Parámetro	Descripción
fileName	Serie opcional. Identifica la ubicación de un solo archivo que se ha de actualizar. Si se omite, se actualizan todas las ubicaciones de archivo de hostName y path.
hostName	Serie necesaria. Identifica el host.
path	Serie necesaria. Para FTP: Especifique el directorio relativo al directorio de inicio de la cuenta de FTP. Para SCP: Especifique el directorio como una vía de acceso absoluta.
newHostName	Serie opcional. Cuando se utiliza, especifica el nuevo nombre de host.
newPath	Serie opcional. Cuando se utiliza, especifica la nueva vía de acceso.
user	Serie necesaria. Cuenta de usuario para acceder al host.
password	Serie necesaria. La contraseña del usuario.
retention	Entero opcional. El número de días que esta entrada se va a conservar en el catálogo (el valor predeterminado es 365).
storageSystem	Serie opcional. Utilice uno de los siguientes: EMC CENTERA, FTP, SCP, TSM.

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi update_entry_location  fileName=a1.corp.com-1_4_2008-01-10_10:27:24.res.70.tar.gz.enc path=/mnt/nfs/ogazit/archive_results/
hostName=qaserver    storageSystem=SCP newPath=/var/dump/mojgan  newHostName=192.168.1.18
```

Tema principal: Referencia de GuardAPI

Funciones de clasificación de GuardAPI

Utilice los siguientes mandatos GuardAPI para la configuración de política de clasificación, para la automatización de pruebas y para scripts de preparación de datos de requisito previo.

Para obtener instrucciones sobre cómo utilizar los mandatos de GuardAPI, consulte el tema de ayuda Visión general de referencia de GuardAPI.

create_classifier_action

Tabla 1. create_classifier_action

Parámetro	Descripción
actionName	Necesario. Serie
actualMemberContent	Necesario. Serie

Parámetro	Descripción
actionType	Necesario. Serie Como referencia, la siguiente es la lista de tipos de acciones con los parámetros necesarios asociados. De este modo, en función de lo que seleccione el usuario para el tipo de acción, se determinan qué parámetros son necesarios. add_to_group_objects actionName - Serie - necesario actualMemberContent - Serie - necesario objectGroup - Serie - necesario policyName - Serie - necesario ruleName - Serie - necesario add_to_group_object_fields actionName - Serie - necesario objectFieldGroup - Serie - necesario policyName - Serie - necesario ruleName - Serie - necesario create_access_rule accessPolicy - Serie - necesario accessRuleAction - Serie - necesario actionName - Serie - necesario ruleName - Serie - necesario create_privacy_set actionName - Serie - necesario policyName - Serie - necesario privacySet - Serie - necesario ruleName - Serie - necesario log_policy_violation actionName - Serie - necesario policyName - Serie - necesario ruleName - Serie - necesario action_send_alert actionName - Serie - necesario policyName - Serie - necesario receiver - Serie - necesario ruleName - Serie - necesario
description	Serie
objectGroup	Necesario. Serie
policyName	Necesario. Serie
ruleName	Necesario. Serie
replaceGroupContent	Booleano
objectFieldGroup	Necesario. Serie
accessPolicy	Necesario. Serie
accessPolicy	Necesario. Serie
accessRuleAction	Necesario. Serie
commandsGroup	Serie
includeField	Booleano
includeServerIP	Booleano
receiver	Serie
privacySet	Necesario. Serie

Parámetro	Descripción
severity	Serie
notificationType	Serie
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplos

```
grdapi create_classifier_action actionType=add_to_group_objects policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc
objectGroup="DW All Objects" replaceGroupContent=1 actualMemberContent=%FULLLIKE

grdapi create_classifier_action actionType=add_to_group_object_fields policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc objectFieldGroup="DW All Object-Field" replaceGroupContent=1

grdapi create_classifier_action actionType=create_access_rule policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc
accessPolicy=pci accessRuleAction="alert daily" commandsGroup="Select command" includeField=1 includeServerIP=0
receiver="syslog,snmp,mail=admin,mail=a b c,custm=-b"

grdapi create_classifier_action actionType=create_privacy_set policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc
privacySet=-b

grdapi create_classifier_action actionType=log_policy_violation policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc
severity=MED

grdapi create_classifier_action actionType=send_alert policyName=-policy1 ruleName=-rule1 actionName=-action1 description=desc
notificationType=High receiver="syslog,snmp,mail=admin,mail=a b c,custm=-b"
```

Valores de los mandatos GuardAPI

Consulte la tabla para obtener una lista de los valores del mandato GuardAPI grdapi create_classifer_action que se utiliza en la GUI. Utilice estos valores para crear grupos.

Tabla 2. GrdAPI create_classifer_action

Valores de la GUI	Valores de GrdAPI
%/%.Name	%/NAME
%/Full	%/FULL
Change/%.Name	CHANGE/NAME
Change/Full	CHANGE/FULL
Nombre completo (Schema.Object)	FULLNAME
Like %Full	%FULLLIKE
Like %Full%	%FULLLIKE%
Like %Name	%NAMELIKE
Like %Name%	%NAMELIKE%
Like Full%	FULLLIKE%
Like Name%	NAMELIKE%
Solo nombre de objeto	NAMEONLY
Read/%.Name	READ/NAME
Read/Full	READ/FULL

Ejemplo

```
grdapi create_classifier_action actionName=classgrpobjectseach1 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent=NAMEONLY description="object type NAMEONLY"
```

Ejemplos de tipos de objetos de grupo

```
grdapi create_group appid=Classifier type=OBJECTS desc="Classifier Group of Each Objects" owner=admin category=classifier
classification=classifier subtype=classifier

grdapi create_datasource type="Oracle (DataDirect)" user=scott password=tiger host="swan.guard.swg.usma.ibm.com"
name="Swan Oracle Object Each" shared=true owner=admin application=Classifier port=1521 serviceName=on8swan0
```

```
grdapi create_classifier_policy policyName="A Group Object Each Type Policy" category="Object Each Process"
classification="Object Each Process"

grdapi create_classifier_rule policyName="A Group Object Each Type Policy" category="Object Each Process"
classification="Object Each Process" ruleName=groupobjects1 ruleType=SEARCH_FOR_DATA dataTypes=TEXT continueOnMatch=1
tableNameLike="EMP_INFORMATION"
columnNameLike="PHONE" tableTypeTable=1

grdapi create_classifier_action actionName=classgrpobjectseach1 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent=NAMEONLY description="object type NAMEONLY"

grdapi create_classifier_action actionName=classgrpobjectseach2 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent=FULLNAME description="object type FULLNAME"

grdapi create_classifier_action actionName=classgrpobjectseach3 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="%NAMELIKE" description="object type %NAMELIKE"

grdapi create_classifier_action actionName=classgrpobjectseach4 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="NAMELIKE%" description="object type NAMELIKE%"

grdapi create_classifier_action actionName=classgrpobjectseach5 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="%NAMELIKE%" description="object type %NAMELIKE%"

grdapi create_classifier_action actionName=classgrpobjectseach6 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="%FULLLIKE" description="object type %FULLLIKE"

grdapi create_classifier_action actionName=classgrpobjectseach7 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="FULLLIKE%" description="object type FULLLIKE%"

grdapi create_classifier_action actionName=classgrpobjectseach8 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="%FULLLIKE%" description="object type %FULLLIKE%"

grdapi create_classifier_action actionName=classgrpobjectseach9 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="Change/Full" description="object type Change/Full"

grdapi create_classifier_action actionName=classgrpobjectseach10 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="CHANGE/NAME" description="object type Change/%.name"

grdapi create_classifier_action actionName=classgrpobjectseach11 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="Read/Full" description="object type Read/Full"

grdapi create_classifier_action actionName=classgrpobjectseach12 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="READ/NAME" description="object type Read/%.name"

grdapi create_classifier_action actionName=classgrpobjectseach13 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="%/Full" description="object type %/Full"

grdapi create_classifier_action actionName=classgrpobjectseach14 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="%/NAME" description="object type %/%.name"

grdapi create_classifier_process policyName="A Group Object Each Type Policy"
processName="A Group Object Each Type Process" datasourceNames="Swan Oracle Object Each"

grdapi create_classifier_action actionName=classgrpobjectseach10 actionType=ADD_TO_GROUP_OBJECTS
policyName="A Group Object Each Type Policy" ruleName=groupobjects1 commandsGroup=groupofobjects
objectGroup="Classifier Group of Each Objects" actualMemberContent="FULLNAME" description="Fully Qualified Name(Schema.Object)
```

create_classifier_policy

Tabla 3. create_classifier_policy

Parámetro	Descripción
category	Necesario. Serie
classification	Necesario. Serie
description	Serie
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi create_classifier_policy policyName=-policy1 classification=class1 description=desc1 category=cat1
```

create_classifier_process

create_classifier_process

Nota: Cree una política de clasificación y un origen de datos antes de invocar esta GuardAPI.

Tabla 4. create_classifier_process

Parámetro	Descripción
comprehensive	Booleano
datasourceNames	Necesario. Serie
includeInternalTables	Booleano. De forma predeterminada, el valor está inhabilitado. Si se habilita includeInternalTables, indica que desea explorar las bases de datos internas del sistema y el esquema que utiliza el proveedor de software de base de datos. Es poco probable que las bases de datos internas del y el esquema contengan datos confidenciales y no se escanean de forma predeterminada. Cuando incluya tablas internas, compruebe que el usuario del origen de datos del clasificador tenga privilegios suficientes para escanear las bases de datos internas y el esquema. Si los privilegios no son suficientes se pueden generar errores de política de clasificación imprevistos. Para ver y editar las bases de datos y el esquema afectados por el parámetro includeInternalTables, utilice el Creador de grupos para editar uno de los grupos de Clasificación excluida predefinidos.
policyName	Necesario. Serie
processName	Necesario. Serie
sampleSize	Entero
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi create_classifier_process  datasourceNames=sample_cls_0001 policyName=APITEST_Cls_Ply_10001_1
processName=APITEST_Clps_10001_1
```

create_classifier_rule

Tabla 5. create_classifier_rule

Parámetro	Descripción
policyName	Necesario. Serie
ruleName	Necesario. Serie

Parámetro	Descripción
ruleType	Necesario. Serie Como referencia, la siguiente es la lista de tipos de reglas válidas con los parámetros necesarios asociados. En función de lo que seleccione el usuario para el tipo de regla, se determinan qué parámetros son necesarios catalog_search_add policyName - Serie - necesario ruleName - Serie - necesario search_by_permissions_add policyName - Serie - necesario ruleName - Serie - necesario grantTypes - Serie - necesario search_for_data_add policyName - Serie - necesario ruleName - Serie - necesario search_for_unstructured_data_add policyName - Serie - necesario ruleName - Serie - necesario
category	Serie
classification	Serie
continueOnMatch	Booleano
description	Serie
columnNameLike	Serie
fireOnlyWithMarker	Serie
tableNameLike	Serie
tableTypeSynonym	Booleano
tableTypeSystemTable	Booleano
tableTypeTable	Booleano
tableTypeView	Booleano
grantTypes	Serie
role	Serie
roleGroup	Serie
user	Serie
userGroup	Serie
withAdminOption	Booleano
compareToValuesInGroup	Serie
compareToValuesInSQL	Serie
dataTypes	Serie
evaluationName	Serie
hitPercentage	Entero
maxLength	Entero
minLength	Entero
searchExpression	Serie
searchLike	Serie
grantTypes	Serie
showUniqueValues	True o False
uniqueValueMask	Valor

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplos

```
grdapi create_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=CATALOG_SEARCH continueOnMatch=1 tableTypeTable=1 tableTypeSynonym=1 tableTypeSystemTable=1 tableTypeView=1
tableNameLike=t1
columnNameLike=c1 fireOnlyWithMarker=m1

grdapi create_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=SEARCH_BY_PERMISSIONS continueOnMatch=1 tableTypeTable=1 tableTypeSynonym=1 tableTypeSystemTable=1 tableTypeView=1
user=user1
userGroup="suspicious users" role=role1 roleGroup=-role1 withAdminOption=1 grantTypes=CONTROL,DELETE,DROP fireOnlyWithMarker=m1

grdapi create_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=SEARCH_FOR_DATA continueOnMatch=1 tableTypeSynonym=1 tableNameLike=tl1 dataTypes=DATE,NUMBER,TEXT columnNameLike=cl1
minLength=11 searchLike=sel1 searchExpression=se1 evaluationName=en1 hitPercentage=44 compareToValuesInSQL=cv1sql
compareToValuesInGroup="dw all objects" fireOnlyWithMarker=m1

grdapi create_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=SEARCH_FOR_UNSTRUCTURED_DATA continueOnMatch=1 searchLike=s1 searchExpression=e1 fireOnlyWithMarker=m1

grdapi create_datasource type="Oracle (DataDirect)" user=scott password=tiger host="swan.guard.swg.usma.ibm.com"
name="Swan Oracle8 all values" shared=true owner=admin application=Classifier port=1521 serviceName=on8swan0

grdapi create_group appid=Classifier type=OBJECTS desc="AA Classifier ALL Values" owner=admin category=classifier
classification=classifier subtype=classifier

grdapi create_member_to_group_by_desc desc="AA Classifier ALL Values" member=ACCOUNTING

grdapi create_member_to_group_by_desc desc="AA Classifier ALL Values" member=ACCOUNTTING

grdapi create_member_to_group_by_desc desc="AA Classifier ALL Values" member=ACCOUNTTING

grdapi create_member_to_group_by_desc desc="AA Classifier ALL Values" member=AG

grdapi create_classifier_policy policyName="Search ALL DATA SEARCH smoke values" category="ALL" classification="ALL"

grdapi create_classifier_rule policyName="Search ALL DATA SEARCH smoke values" category="ALL" classification=ALL
ruleName=ALL1 ruleType=SEARCH_FOR_DATA dataTypes=TEXT,NUMBER continueOnMatch=1 tableNameLike="DEPT14%" minLength=1 maxLength=100
tableTypeSynonym=1 tableTypeSystemTable=1 tableTypeTable=1 tableTypeView=1 fireOnlyWithMarker=ACCT searchLike="A%"
searchExpression="^AA*" columnNameLike="DNAME" evaluationName="com.guardium.classifier.custom.RichardEvaluation" hitPercentage=10
compareToValuesInGroup="AA Classifier ALL Values" compareToValuesInSQL="select DNAME from SCOTT.DEPT where DNAME like 'A%G'"
showUniqueValues="true" uniqueValueMask="^AA*"

grdapi create_classifier_process policyName="Search ALL DATA SEARCH smoke values"
processName="Search ALL DATA SEARCH smoke values Process" datasourceNames="Swan Oracle8 all values"
```

delete_classifier_action

Tabla 6. delete_classifier_action

Parámetro	Descripción
actionName	Necesario. Serie
policyName	Necesario. Serie

Ejemplo

```
grdapi delete_classifier_action policyName=-policy1 ruleName=-rule1 actionName=-action1
```

delete_classifier_policy

Tabla 7. delete_classifier_policy

Parámetro	Descripción
policyName	Necesario. Serie

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi delete_classifier_policy policyName=-policy1
```

delete_classifier_process

Tabla 8. list_classifier_process

Parámetro	Descripción
processName	Serie
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

ejemplo

```
grdapi delete_classifier_process processName=APITEST_Clps_10001_1
```

delete_classifier_rule

Tabla 9. delete_classifier_rule

Parámetro	Descripción
policyName	Necesario. Serie
ruleName	Necesario. Serie
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi delete_classifier_rule policyName=-policy1 ruleName=-rule1
```

execute_cls_process

Ejecutar (enviar) un proceso de clasificación

Ejecuta un proceso de clasificación. Es equivalente a Ejecutar una vez ahora en el Creador de procesos de clasificación. Envía el trabajo que coloca el proceso en la cola de trabajos de Guardium, desde la que el dispositivo ejecuta un solo trabajo cada vez. Los administradores pueden ver el estado del trabajo seleccionado Supervisor de Guardium > Cola de trabajos de Guardium.

Nota: Cree un proceso de clasificación antes de invocar esta API.

Tabla 10. execute_cls_process

Parámetro	Descripción

Parámetro	Descripción
processName	Nombre del proceso de clasificación
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi execute_cls_process processName="classPolicy1"
```

La siguiente es una lista de funciones del clasificador y los parámetros para cada una de ellas. En el caso de que el parámetro tenga una lista de entradas válidas suministrada, se proporciona la lista.

list_classifier_policies

Tabla 11. list_classifier_policies

Parámetro	Descripción
policyName	Necesario. Serie
ruleName	Necesario. Serie
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi list_classifier_policy policyName=-policy1 ruleName=-rule1 actionName=-action1 recursive=1
```

Nota: Si se ejecuta esta función sin ningún argumento se listan todas las políticas. Si se pasa un argumento para la política, se listan todas las reglas y acciones para la política. Si se pasa una política y una regla se listan todas las acciones para la regla.

list_classifier_process

Tabla 12. list_classifier_process

Parámetro	Descripción
processName	Serie
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

ejemplo:

grdapi list_classifier_process processName=APITEST_CLPS_30001

set_classification_concurrency_limit

El mandato set_classification_concurrency_limit define el número de procesos del clasificador que se pueden ejecutar simultáneamente.

Sintaxis: grdapi set_classification_concurrency_limit limit=[value].

Tabla 13. Parámetros de set_classification_concurrency_limit

Parámetro	Valor	Descripción
limit	Entero: 1-100, en función de la configuración de hardware del sistema Guardium. El valor predeterminado es 1.	El valor de limit define el número de procesos del clasificador que se pueden ejecutar simultáneamente. El valor de limit es el valor menor que 100 o dos veces el número de núcleos de CPU instalados en el sistema Guardium. Por ejemplo, si un sistema tiene 8 núcleos de CPU, el valor máximo de limit es 16. Si un sistema tiene 64 núcleos de CPU, el valor máximo de limit es 100. El valor predeterminado de limit es 1.

Ejemplo:

```
grdapi set_classification_concurrency_limit limit=11
```

Mostrar valores: grdapi get_classification_concurrency_limit

update_classifier_action

Tabla 14. update_classifier_action

Parámetro	Descripción
actionName	Necesario. Serie
actualMemberContent	Necesario. Serie
description	Serie
objectGroup	Necesario. Serie
policyName	Necesario. Serie
ruleName	Necesario. Serie
replaceGroupContent	Booleano
objectFieldGroup	Necesario. Serie
accessPolicy	Necesario. Serie
accessRuleAction	Necesario. Serie
commandsGroup	Serie
includeField	Booleano
includeServerIP	Booleano
receiver	Serie
privacySet	Necesario. Serie
severity	Serie
notificationType	Serie
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi update_classifier_action actionType=add_to_group_objects policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc objectGroup="DW All Objects" replaceGroupContent=1 actualMemberContent=%FULLLIKE

grdapi update_classifier_action actionType=add_to_group_object_fields policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc objectFieldGroup="DW All Object-Field" replaceGroupContent=1

grdapi update_classifier_action actionType=update_access_rule policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc accessPolicy=pci accessRuleAction="alert daily" commandsGroup="Select command" includeField=1 includeServerIP=0
receiver="syslog,snmp,mail=admin,mail=a b c,custm=-b"

grdapi update_classifier_action actionType=update_privacy_set policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc privacySet=-b

grdapi update_classifier_action actionType=log_policy_violation policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc severity=MED

grdapi update_classifier_action actionType=send_alert policyName=-policy1 ruleName=-rule1 actionName=-action1
description=desc notificationType=High receiver="syslog,snmp,mail=admin,mail=a b c,custm=-b"
```

update_classifier_policy

Tabla 15. update_classifier_policy

Parámetro	Descripción
policyName	Necesario. Serie
category	Necesario. Serie
classification	Necesario. Serie
description	Serie
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi update_classifier_policy policyName=-policy1 classification=class1 description=desc1 category=cat1
```

update_classifier_process

update_classifier_process

Tabla 16. update_classifier_process

Parámetro	Descripción
comprehensive	Booleano
datasourceNames	Necesario. Serie
includeInternalTables	Booleano. De forma predeterminada, el valor está inhabilitado. Si se habilita includeInternalTables, indica que desea explorar las bases de datos internas del sistema y el esquema que utiliza el proveedor de software de base de datos. Es poco probable que las bases de datos internas del y el esquema contengan datos confidenciales y no se escanean de forma predeterminada. Cuando incluya tablas internas, compruebe que el usuario del origen de datos del clasificador tenga privilegios suficientes para escanear las bases de datos internas y el esquema. Si los privilegios no son suficientes se pueden generar errores de política de clasificación imprevistos. Para ver y editar las bases de datos y el esquema afectados por el parámetro includeInternalTables, utilice el Creador de grupos para editar uno de los grupos de Clasificación excluida predefinidos.
newName	Serie
policyName	Necesario. Serie
processName	Necesario. Serie
sampleSize	Entero
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi update_classifier_process datasourceNames=sample_cls_0001,sample_cls_0002 policyName=APITEST_Cls_Ply_10001_1 processName=APITEST_Clps_10001_1 comprehensive=0 sampleSize=3000

update_classifier_rule

Tabla 17. update_classifier_rule

Parámetro	Descripción
policyName	Necesario. Serie
ruleName	Necesario. Serie

Parámetro	Descripción
ruleType	Necesario. Serie valores– catalog_search search_by_permissions search_for_data search_for_unstructured_data
category	Serie
classification	Serie
continueOnMatch	Booleano
description	Serie
columnNameLike	Serie
fireOnlyWithMarker	Serie
tableNameLike	Serie
tableTypeSynonym	Booleano
tableTypeSystemTable	Booleano
tableTypeTable	Booleano
tableTypeView	Booleano
grantTypes	Serie
role	Serie
roleGroup	Serie
user	Serie
userGroup	Serie
withAdminOption	Booleano
compareToValuesInGroup	Serie
compareToValuesInSQL	Serie
dataTypes	Serie
evaluationName	Serie
hitPercentage	Entero
maxLength	Entero
minLength	Entero
searchExpression	Serie
searchLike	Serie
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplos

```
grdapi update_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=CATALOG_SEARCH continueOnMatch=1 tableTypeTable=1 tableTypeSynonym=1 tableTypeSystemTable=1 tableTypeView=1
tableNameLike=t1
columnNameLike=c1 fireOnlyWithMarker=m1

grdapi update_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=SEARCH_BY_PERMISSIONS continueOnMatch=1 tableTypeTable=1 tableTypeSynonym=1 tableTypeSystemTable=1 tableTypeView=1
user=user1
userGroup="suspicious users" role=role1 roleGroup=-role1 withAdminOption=1 grantTypes=CONTROL,DELETE,DROP fireOnlyWithMarker=m1

grdapi update_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=SEARCH_FOR_DATA continueOnMatch=1 tableTypeSynonym=1 tableNameLike=tl1 dataTypes=DATE,NUMBER,TEXT columnNameLike=cl1
minLength=11
maxLength=22 searchLike=sel1 searchExpression=se1 evaluationName=en1 hitPercentage=44 compareToValuesInSQL=cv1sql
compareToValuesInGroup="dw all objects" fireOnlyWithMarker=m1

grdapi update_classifier_rule policyName=-policy1 ruleName=-rule1 category=-cat1 classification=-class1 description=-desc1
ruleType=SEARCH_FOR_UNSTRUCTURED_DATA continueOnMatch=1 searchLike=s1 searchExpression=e1 fireOnlyWithMarker=m1
```

Funciones de orígenes de datos de GuardAPI Cloud

Utilice este mandato para definir un origen de datos de nube.

create_cloud_datasource

Parámetro	Tipo de valor	Descripción
application	Serie. Consulte la descripción	Necesario. La aplicación para la que se está definiendo el origen de datos. Uno de los valores siguientes: Política de acceso Conversión de usuarios de aplicación Tarea de auditoría Sistema de auditoría de cambios Clasificador Dominio personalizado Analizador de bases de datos Valores de supervisor Asesoramiento de seguridad Verificación de stap
cloudTitle	Serie. Consulte la descripción	Necesario. El nombre de la cuenta de nube que ya está definida en Guardium
compatibilityMode	Serie	El modo utilizado para la supervisión de una tabla.
conProperty	Serie	Opcional. Utilícelo sólo si se deben incluir propiedades de conexión adicionales en el URL de JDBC para establecer una conexión JDBC con este origen de datos. El formato requerido es propiedad=valor, donde cada par de propiedad y valor se ha de separar del siguiente con una coma.
customURL	Serie	Opcional. La serie de conexión con el origen de datos. De lo contrario, la conexión se realiza utilizando el host, puerto, instancia, propiedades, etc. de los campos especificados previamente. Esto resulta útil para crear conexiones OID (Oracle Internet Directory).
dbInstanceAccount	Serie	Opcional. Nombre de inicio de sesión de cuenta de base de datos que utiliza CAS
dbInstanceDirectory	Serie	Opcional. El directorio donde se ha instalado el software de base de datos que utiliza CAS
dbName	Serie	Opcional. Para un origen de datos DB2 u Oracle, entre el nombre de esquema. Para otros, especifique el nombre de la base de datos.
description	Serie	Opcional. La descripción larga del origen de datos.
host	Serie	Necesario. El nombre de host o la dirección IP.
importServerSSLcert	Booleano	
KerberosConfigName	Serie	Opcional. El nombre de la configuración de Kerberos que ya está definida en el sistema Guardium
name	Serie	Necesario. Un nombre exclusivo para el origen de datos en el sistema Guardium.
objectLimit	0, entero positivo	Necesario. El número máximo de objetos confidenciales encontrados en el proceso de clasificación que se añaden automáticamente a la lista de objetos auditados. Valor predeterminado = 20.
password	serie	La contraseña del usuario.
port	Entero	Opcional. Número de puerto.
primaryCollector	Entero	El recopilador que extrae los datos de auditoría de la base de datos en la nube.
region	lista de valores	Necesario.
savePassword	Booleano	Guarda y cifra sus credenciales de autenticación en el dispositivo Guardium. Es necesario si está definiendo un origen de datos con una aplicación que se ejecuta como una tarea planificada (en oposición a bajo demanda). Si se establece en yes, se requiere el nombre de inicio de sesión y la contraseña.
serviceName	Serie	Opcional. Necesario para Oracle, Informix, DB2 e IBM ISeries. Para un origen de datos de DB2, escriba el nombre de base de datos, para otros, especifique el nombre de servicio.
severity	Serie - Lista de valores de constantes	Opcional. La clasificación de gravedad (o el nivel de impacto) del origen de datos. Uno de los siguientes: LOW NONE MED HIGH

Parámetro	Tipo de valor	Descripción
shared	Serie - Lista de valores de constantes	Opcional. Se establece en **True** o **Share** para compartirlo con otras aplicaciones. Para compartir el origen de datos con otros usuarios, se han de asignar roles desde la GUI. Valores: Share Not Shared True False
type	lista de valores	Necesario. Identifica el tipo de origen de datos. Valores válidos: Oracle (DataDirect - SID) Oracle (DataDirect - Nombre de servicio)
useKerberos	Booleano	Opcional (booleano). Se establece en sí para utilizar la autenticación de Kerberos. Si es sí, se debe proporcionar KerberosConfigName.
useLDAP	Booleano	Opcional (booleano). Se establece en sí para utilizar LDAP.
user	Serie	Opcional. El usuario del origen de datos. Si se utiliza, también se debe utilizar la contraseña.
useSSL	Booleano	Opcional (booleano). Se establece en sí para utilizar la autenticación de SSL.

list_cloud_datasource_by_name

Parámetro	Tipo de valor	Descripción
name	serie	Necesario. Nombre de origen de datos de nube definido en Guardium.
api_target_host	serie	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM)

restart_cloud_instance

Reinicia la instancia de nube especificada.

Parámetro	Tipo de valor	Descripción
datasource_name	serie	Necesario. Nombre de origen de datos de nube definido en Guardium.
api_target_host	serie	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM)

update_cloud_datasource

Actualiza la configuración del origen de datos de nube.

Parámetro	Tipo de valor	Descripción
cloudTitle	Serie. Lista de valores de constantes	Necesario. El título definido por el mandato GRDAPI
conProperty	Serie	Opcional. Utilícelo sólo si se deben incluir propiedades de conexión adicionales en el URL de JDBC para establecer una conexión JDBC con este origen de datos. El formato requerido es propiedad=valor, donde cada par de propiedad y valor se ha de separar del siguiente con una coma.
customURL	Serie	Opcional. La serie de conexión con el origen de datos. De lo contrario, la conexión se realiza utilizando el host, puerto, instancia, propiedades, etc. de los campos especificados previamente. Esto resulta útil para crear conexiones OID (Oracle Internet Directory).
dbInstanceAccount	Serie	Opcional. Nombre de inicio de sesión de cuenta de base de datos que utiliza CAS
dbInstanceDirectory	Serie	Opcional. El directorio donde se ha instalado el software de base de datos que utiliza CAS

Parámetro	Tipo de valor	Descripción
dbName	Serie	Opcional. Para un origen de datos DB2 u Oracle, entre el nombre de esquema. Para otros, especifique el nombre de la base de datos.
description	Serie	Opcional. La descripción larga del origen de datos.
host	Serie	Necesario. El nombre de host o la dirección IP.
importServerSSLcert	Booleano	
KerberosConfigName	Serie	El nombre de la configuración de Kerberos que ya está definida en el sistema Guardium
name	Serie	Necesario. Un nombre exclusivo para el origen de datos en el sistema Guardium.
newName		
objectLimit	entero: 0 y superior	Necesario. El número máximo de objetos confidenciales encontrados en el proceso de clasificación que se añaden automáticamente a la lista de objetos auditados.
password		La contraseña del usuario.
port	Entero	Nombre de origen de datos de nube definido en Guardium.
primaryCollector	Entero	El recopilador que recibe los datos desde la BD en la nube
region	lista de valores	Necesario.
savePassword	Booleano	Guarda y cifra sus credenciales de autenticación en el dispositivo Guardium. Es necesario si está definiendo un origen de datos con una aplicación que se ejecuta como una tarea planificada (en oposición a bajo demanda). Si se establece en yes, se requiere el nombre de inicio de sesión y la contraseña.
serviceName	Serie	Opcional. Necesario para Oracle, Informix, DB2 e IBM ISeries. Para un origen de datos de DB2, escriba el nombre de base de datos, para otros, especifique el nombre de servicio.
severity	Serie - Lista de valores de constantes	Opcional. La clasificación de gravedad (o el nivel de impacto) del origen de datos. Uno de los siguientes: LOW NONE MED HIGH
shared	Serie - Lista de valores de constantes	Opcional. Se establece en **True** o **Share** para compartirlo con otras aplicaciones. Para compartir el origen de datos con otros usuarios, se han de asignar roles desde la GUI. Valores: Share Not Shared True False
useKerberos	Booleano	Opcional (booleano). Se establece en sí para utilizar la autenticación de Kerberos. Si es sí, se debe proporcionar KerberosConfigName.
useLDAP	Booleano	Opcional (booleano). Se establece en sí para utilizar LDAP.
user	Serie	Opcional. El usuario del origen de datos. Si se utiliza, también se debe utilizar la contraseña.
useSSL	Booleano	Opcional (booleano). Se establece en sí para utilizar la autenticación de SSL.

Tema principal: Referencia de GuardAPI

Funciones de usuario de base de datos de GuardAPI

Utilice estos mandatos de GuardAPI para mantener la correlación de los usuarios de la base de datos, la exploración no de credenciales y establecer el nivel de depuración.

non_credential_scan

API que permite someter trabajos que explorarán las bases de datos de serversGroup para los usuarios predeterminados habilitados en usersGroup. Los trabajos enviados se ejecutan bajo el escucha de clasificador y se pueden rastrear utilizando el informe Cola de trabajos de clasificador/asesoramiento. Se puede cancelar un trabajo sometido desde el informe Cola de trabajos de clasificador/asesoramiento, pulsando dos veces el trabajo y seleccionando Detener trabajo.

Nota: Si no se puede acceder a un servidor en serversGroup, se añade una excepción de tipo Excepción de trabajo planificado y el servidor no se escanea.

Tabla 1. non_credential_scan

Parámetro	Descripción
databaseType	Necesario. Debe ser uno de las siguientes: ORACLE, DB2, SYBASE, MS SQL SERVER, MYSQL, TERADATA, POSTGRESQL, NETEZZA, IBM ISERIES, INFORMIX
serversGroup	Necesario. Debe ser un grupo de servidores válido (IP Servidor/Nombre de instancia/Puerto), como se ha definido con el creador de grupos.
usersGroup	Necesario. Debe ser un grupo de usuarios válido (Usuario BD/Contraseña BD), como se ha definido con el creador de grupos. En el creador de grupos existen grupos predeterminados.

Ejemplo

```
grdapi non_credential_scan databaseType=ORACLE serversGroup=oracleServers usersGroup="ORACLE Default Users"
```

Mantener correlación de base de datos

Estas API ayudan a mantener la correlación entre los usuarios de base de datos (invocadores de código SQL que ha causado una infracción) y las direcciones de correo electrónico para alertas en tiempo real. Consulte la sección Acciones de alertas, para obtener más información sobre los invocadores.

- create_db_user_mapping
- delete_db_user_mapping
- list_db_user_mapping

create_db_user_mapping

Uso de comodines:

- En los mandatos 'delete' y 'list', los 4 parámetros aceptan comodines ('%')
- Mandato 'create':
  - serverIp: El comodín es válido, se puede incluir '%' en lugar del número en el formato de ip_address
  - 192.168.2.%: Válido
  - 192.%.2.%: Válido
  - 192.%: No válido
- serviceName: Se permiten comodines (%)
- dbUserName: Sin comodines. '%' es válido pero se considerará como el símbolo '%'
- emailAddress: Sin comodines. '%' es válido pero se considerará como el símbolo '%'

Tabla 2. create_db_user_mapping

Parámetro	Descripción
serverIp	Necesario (Dirección IP). Debe tener el formato de una dirección IP A.B.C.D
serviceName	Necesario (cualquier serie). Identifica el nombre de servicio.
dbUserName	Necesario (cualquier serie). Identifica el nombre de usuario de base de datos.
emailAddress	Necesario (cualquier serie y requiere un signo '@'). Identifica la dirección de correo electrónico.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi create_db_user_mapping serverIp=192.168.1.104 serviceName=ora1 dbUserName=scott emailAddress=scott@oracle.com
```

delete_db_user_mapping

Uso de comodines:

- En los mandatos 'delete' y 'list', los 4 parámetros aceptan comodines ('%')
- Mandato 'create':
  - serverIp: El comodín es válido, se puede incluir '%' en lugar del número en el formato de ip_address
  - 192.168.2.%: Válido
  - 192.%.2.%: Válido
  - 192.%: No válido
- serviceName: Se permiten comodines (%)
- dbUserName: Sin comodines. '%' es válido pero se considerará como el símbolo '%'
- emailAddress: Sin comodines. '%' es válido pero se considerará como el símbolo '%'

Tabla 3. delete_db_user_mapping

Parámetro	Descripción
serverIp	Necesario (Dirección IP). Debe tener el formato de una dirección IP A.B.C.D
serviceName	Necesario (cualquier serie). Identifica el nombre de servicio.
dbUserName	Necesario (cualquier serie). Identifica el nombre de usuario de base de datos.
emailAddress	Necesario (cualquier serie y requiere un signo '@'). Identifica la dirección de correo electrónico.

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi create_db_user_mapping serverIp=192.168.1.104 serviceName=ora1 dbUserName=scott emailAddress=scott@oracle.com
```

list_db_user_mapping

Uso de comodines:

- En los mandatos 'delete' y 'list', los 4 parámetros aceptan comodines ('%')
- Mandato 'create':
  - serverIp: El comodín es válido, se puede incluir '%' en lugar del número en el formato de ip_address
  - 192.168.2.%: Válido
  - 192.%.2.%: Válido
  - 192.%: No válido
- serviceName: Se permiten comodines (%)
- dbUserName: Sin comodines. '%' es válido pero se considerará como el símbolo '%'
- emailAddress: Sin comodines. '%' es válido pero se considerará como el símbolo '%'

Tabla 4. list_db_user_mapping

Parámetro	Descripción
serverIp	Necesario (Dirección IP). Debe tener el formato de una dirección IP A.B.C.D
serviceName	Necesario (cualquier serie). Identifica el nombre de servicio.
dbUserName	Necesario (cualquier serie). Identifica el nombre de usuario de base de datos.
emailAddress	Necesario (cualquier serie y requiere un signo '@'). Identifica la dirección de correo electrónico.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi create_db_user_mapping serverIp=192.168.1.104 serviceName=ora1 dbUserName=scott emailAddress=scott@oracle.com
```

get debug level

Utilice este mandato de GuardAPI para ver el nivel de depuración de la salida de IMS.

set_debug_level

Utilice este mandato de GuardAPI para controlar la salida de IMS.

Si IMS debug_level = 1, La salida de los campos de depuración de IMS, como mvs_is_plex, mvs_ipaddr, mvs_dlta_sign, mvs_dlta_val se realizará en las tablas de base de datos internas, GDM_CONSTRUCT_TEXT.FULL_SQL o GDM_EXCEPTION.FULL_SQL. Si el nivel de depuración de IMS es 0, no se distribuirán los campos de depuración de IMS.

Tema principal: Referencia de GuardAPI

Funciones de orígenes de datos de GuardAPI

Utilice estos mandatos GuardAPI para crear, listar, suprimir y actualizar funciones de origen de datos.

create_datasource

Utilice este mandato para definir un nuevo origen de datos.

Nota: En el entorno del Gestor central, los orígenes de datos se definen en el Gestor central. GuardAPI le permite crear orígenes de datos en una unidad gestionada, pero estos orígenes de datos no se pueden ver ni utilizar.

Para crear orígenes de datos en la nube, consulte Funciones de orígenes de datos de GuardAPI Cloud.

Tabla 1. create_datasource

Parámetro	**Descripción**
application	Necesario. Identifica la aplicación para la que se está definiendo el origen de datos. Debe ser uno de los valores siguientes: Access_policy Conversión de usuarios de aplicación AuditDatabase AuditTask ChangeAuditSystem Clasificador CustomDomain DatabaseAnalyzer MonitorValues SecurityAssessment Stap_Verification
compatibilityMode	Modo de compatibilidad: Las opciones son Valor predeterminado o MSSQL 2000. Se indica al procesador la modalidad de compatibilidad que se ha de utilizar cuando se supervisa una tabla.
conProperty	Opcional. Utilícelo sólo si se deben incluir propiedades de conexión adicionales en el URL de JDBC para establecer una conexión JDBC con este origen de datos. El formato requerido es propiedad=valor, donde cada par de propiedad y valor se ha de separar del siguiente con una coma. Para una base de datos Sybase con un conjunto de caracteres predeterminado de Roman8, especifique la propiedad siguiente: charSet = utf8
customURL	Opcional. La serie de conexión con el origen de datos. De lo contrario, la conexión se realiza utilizando el host, puerto, instancia, propiedades, etc. de los campos especificados previamente. Por ejemplo, esto resulta útil para crear conexiones OID (Oracle Internet Directory).
dbInstanceAccount	Opcional. Nombre de inicio de sesión de cuenta de base de datos que utilizará CAS
dbInstanceDirectory	Opcional. El directorio donde se ha instalado el software de base de datos que utiliza CAS
dbName	Opcional. Para un origen de datos DB2 u Oracle, entre el nombre de esquema. Para otros, especifique el nombre de la base de datos.
description	Opcional. La descripción larga del origen de datos.
host	Necesario. Puede ser el nombre de host o la dirección IP.
KerberosConfigName	Opcional. El nombre de la configuración de Kerberos que ya está definida en el sistema Guardium
name	Necesario. Proporciona un nombre exclusivo para el origen de datos en el sistema.
password	Opcional. La contraseña del usuario.
port	Opcional (entero). Número de puerto.
savePassword	Guarda y cifra sus credenciales de autenticación en el dispositivo Guardium. Es necesario si está definiendo un origen de datos con una aplicación que se ejecuta como una tarea planificada (en oposición a bajo demanda). Si se establece en yes, se requiere el nombre de inicio de sesión y la contraseña.
serviceName	Necesario para Oracle, Informix, DB2 e IBM® ISeries. Para un origen de datos DB2, escriba el nombre de base de datos, para otros, especifique el nombre de servicio.
severity	Opcional. La clasificación de gravedad (o el nivel de impacto) del origen de datos.
shared	Opcional (booleano). Se establece en **true** para compartirlo con otras aplicaciones. Para compartir el origen de datos con otros usuarios, se han de asignar roles desde la GUI.

Parámetro	Descripción
type	Necesario. Identifica el tipo de origen de datos. Valores válidos: DB2 DB2 for i DB2 for z/OS Informix MM SQL Server MS SQL Server (DataDirect) MySQL NA Netezza Oracle (DataDirect) Oracle (Nombre de servicio) Oracle (SID) PostgreSQL Sybase Sybase IQ Teradata Se puede utilizar lo siguiente cuando la aplicación es CustomDomain o Clasificador: TEXT TEXT:FTP TEXT:HTTP TEXT:HTTPS TEXT:SAMBA
useKerberos	Opcional (booleano). Se establece en sí para utilizar la autenticación de Kerberos. Si es sí, se debe proporcionar KerberosConfigName.
useLDAP	Opcional (booleano). Se establece en sí para utilizar LDAP.
user	Opcional. El usuario del origen de datos. Si se utiliza, también se debe utilizar la contraseña.
useSSL	Opcional (booleano). Se establece en sí para utilizar la autenticación de SSL.

Ejemplo

```
grdapi create_datasource type=DB2 name=chickenDB2  password=guardium user=db2inst1 dbName=dn0chick application=Access_policy
shared=true port=50000 host=chicken.corp.com
```

create_test_exception

Utilice este mandato para añadir registros a las excepciones de prueba. Esto afecta al comportamiento de los asesoramientos de vulnerabilidad, si falla una prueba en un origen de datos específico, se comprueba el último registro de la tabla de excepciones de prueba del origen de datos o de la prueba, de modo que si la fecha de ejecución está incluida entre las fechas desde y hasta del último registro de la prueba, se establecerá en PASS. La recomendación se establecerá en la explicación (del registro de excepciones) y el texto del resultado se establecerá en:

```
Test passed, based on exception approved by: .... effective from date to date.
```

Nota: La API solo añade registros para eliminar una excepción, se debe crear un nuevo registro con fechas nuevas, según sea necesario.

Tabla 2. create_test_exception

Parámetro	Descripción
datasourceName	Necesario. Nombre válido de un origen de datos definido.
testDescription	Necesario. Nombre de prueba válido en los asesoramientos de seguridad.
fromDate	Necesario. Fecha de inicio de la validez de la excepción.
toDate	Necesario. Fecha final de la validez de la excepción.
explanation	Necesario. Una recomendación sobre por qué se superará la prueba.

Ejemplo

```
grdapi create_test_exception datasourceName=ORAPROD5 testDescription="CVE-2009-0997" fromDate="2012-07-01 08:00:00" toDate="2012-
07-31 08:00:00" explanation="Currently in testing stage"
```

list_datasource_by_name

Muestra una definición de origen de datos identificado por un nombre.

Tabla 3. list_datasource_by_name

Parámetro	Descripción
name	Necesario. El nombre del origen de datos.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
CLI> grdapi list_datasource_by_name name=chickenDB2
ID=20000
Datasource DatasourceId=20000
Datasource DatasourceTypeId=2
Datasource Name=chickenDB2
Datasource Description=null
Datasource Host=chicken.corp.com
Datasource Port=50000
Datasource ServiceName=
Datasource UserName=db2inst1
Datasource Password=[B@1415de6
Datasource PasswordStored=true
Datasource DbName=dn0chick
Datasource LastConnect=null
Datasource Timestamp=2008-04-18 15:40:58.0
Datasource ApplicationId=2
Datasource Shared=true
Datasource ConProperty=null
Datasource type =DB2
Application Type = Access_policy
ok
```

list_datasource_by_id

Muestra una definición de origen de datos identificado por una clave de ID.

Tabla 4. list_datasource_by_id

Parámetro	Descripción
id	Necesario (entero). Escriba el número de ID del origen de datos que se va a listar.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi list_datasource_by_id id=2
```

delete_datasource_by_name

Suprime la definición del origen de datos especificado, a menos que una aplicación esté utilizando dicho origen de datos. Esta función elimina el origen de datos, independientemente de quién lo haya creado.

Tabla 5. delete_datasource_by_name

Parámetro	Descripción
name	Necesario. El nombre del origen de datos.

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi delete_datasource_by_name name=swanSybase
```

delete_datasource_by_id

Suprime la definición del origen de datos especificado, a menos que una aplicación esté utilizando dicho origen de datos. Esta función elimina el origen de datos, independientemente de quién lo haya creado.

Tabla 6. delete_datasource_by_id

Parámetro	Descripción
id	Necesario (entero). Escriba el número de ID del origen de datos que se va a listar.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi delete_datasource_by_id id=2
```

update_datasource_by_name

Actualiza una definición de origen de datos.

Tabla 7. update_datasource_by_name

Parámetro	Descripción
name	Necesario. Identifica el origen de datos que se va a actualizar.
newName	Opcional. Proporciona un nombre nuevo, que debe ser exclusivo para un origen de datos en el sistema.
description	Opcional. La descripción larga del origen de datos.
host	Opcional. Puede ser el nombre de host o la dirección IP.
port	Opcional (entero). Número de puerto.
savePassword	Guarda y cifra sus credenciales de autenticación en el dispositivo Guardium. Es necesario si está definiendo un origen de datos con una aplicación que se ejecuta como una tarea planificada (en oposición a bajo demanda). Si se establece en yes, se requiere el nombre de inicio de sesión y la contraseña.
serviceName	Opcional. Para un origen de datos Oracle, especifique el nombre de servicio.
user	Opcional. El usuario del origen de datos. Si se utiliza, también se debe utilizar la contraseña.
password	Opcional. La contraseña del usuario. Si se utiliza, también se debe utilizar el usuario.
dbName	Opcional. Para los orígenes de datos de DB2, especifique el nombre de la base de datos.
conProperty	Opcional. Utilícelo sólo si se deben incluir propiedades de conexión adicionales en el URL de JDBC para establecer una conexión JDBC con este origen de datos. El formato requerido es propiedad=valor, donde cada par de propiedad y valor se ha de separar del siguiente con una coma. Para una base de datos Sybase con un conjunto de caracteres predeterminado de Roman8, especifique la propiedad siguiente: CHARSET = utf8
dbInstanceAccount	Opcional. Nombre de inicio de sesión de cuenta de base de datos que utilizará CAS
dbInstanceDirectory	Opcional. El directorio donde se ha instalado el software de base de datos que utiliza CAS

Parámetro	Descripción
shared	Opcional (booleano). Se establece en **true** para compartirlo con otras aplicaciones. Para compartir el origen de datos con otros usuarios, se han de asignar roles desde la GUI.
customURL	Opcional. La serie de conexión con el origen de datos. De lo contrario, la conexión se realiza utilizando el host, puerto, instancia, propiedades, etc. de los campos especificados previamente. Por ejemplo, esto resulta útil para crear conexiones OID (Oracle Internet Directory).
severity	Opcional. La clasificación de gravedad (o el nivel de impacto) del origen de datos.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.
useKerberos	Opcional (booleano). Se establece en sí para utilizar la autenticación de Kerberos. Si es sí, se debe proporcionar KerberosConfigName.
useLDAP	Opcional (booleano). Se establece en sí para utilizar LDAP.
useSSL	Opcional (booleano). Se establece en sí para utilizar la autenticación de SSL.

Ejemplo

```
grdapi update_datasource_by_name name=chickenDB2  newName="chicken DB2" user=" " password=" "
```

update_datasource_by_id

Actualiza una definición de origen de datos.

Tabla 8. update_datasource_by_id

Parámetro	Descripción
id	Necesario (entero). Identifica el origen de datos.
newName	Opcional. Proporciona un nombre nuevo, que debe ser exclusivo para un origen de datos en el sistema.
description	Opcional. La descripción larga del origen de datos.
host	Opcional. Puede ser el nombre de host o la dirección IP.
port	Opcional (entero). Número de puerto.
savePassword	Guarda y cifra sus credenciales de autenticación en el dispositivo Guardium. Es necesario si está definiendo un origen de datos con una aplicación que se ejecuta como una tarea planificada (en oposición a bajo demanda). Si se establece en yes, se requiere el nombre de inicio de sesión y la contraseña.
serviceName	Opcional. Para un origen de datos Oracle, especifique el nombre de servicio.
user	Opcional. El usuario del origen de datos. Si se utiliza, también se debe utilizar la contraseña.
password	Opcional. La contraseña del usuario. Si se utiliza, también se debe utilizar el usuario.
dbName	Opcional. Para los orígenes de datos de DB2, especifique el nombre de la base de datos.
conProperty	Opcional. Utilícelo sólo si se deben incluir propiedades de conexión adicionales en el URL de JDBC para establecer una conexión JDBC con este origen de datos. El formato requerido es propiedad=valor, donde cada par de propiedad y valor se ha de separar del siguiente con una coma. Para una base de datos Sybase con un conjunto de caracteres predeterminado de Roman8, especifique la propiedad siguiente: CHARSET = utf8
dbInstanceAccount	Opcional. Nombre de inicio de sesión de cuenta de base de datos que utilizará CAS
dbInstanceDirectory	Opcional. El directorio donde se ha instalado el software de base de datos que utiliza CAS
shared	Opcional (booleano). Se establece en **true** para compartirlo con otras aplicaciones. Para compartir el origen de datos con otros usuarios, se han de asignar roles desde la GUI.
customURL	Opcional. La serie de conexión con el origen de datos. De lo contrario, la conexión se realiza utilizando el host, puerto, instancia, propiedades, etc. de los campos especificados previamente. Por ejemplo, esto resulta útil para crear conexiones OID (Oracle Internet Directory).
severity	Opcional. La clasificación de gravedad (o el nivel de impacto) del origen de datos.

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.
useKerberos	Opcional (booleano). Se establece en sí para utilizar la autenticación de Kerberos. Si es sí, se debe proporcionar KerberosConfigName.
useLDAP	Opcional (booleano). Se establece en sí para utilizar LDAP.
useSSL	Opcional (booleano). Se establece en sí para utilizar la autenticación de SSL.

Ejemplo

```
grdapi update_datasource_by_id id=20000 user=" " password=" " newName="chickenDB2hooo"
```

list_db_drivers

Ahora está soportado listar solo el nombre de los controladores de base de datos Oracle (DataDirect) y MS SQL SERVER (DataDirect) como tipos de orígenes de datos.

list_db_drivers_by_details

Lista cada controlador de base de datos más detalladamente (nombre, clase, controlador, clase, URL e ID de tipo de origen de datos)

Tema principal: Referencia de GuardAPI

Funciones de referencia de orígenes de datos de GuardAPI

Utilice estos mandatos GuardAPI para crear, listar, suprimir y actualizar funciones de referencia de orígenes de datos.

create_datasourceRef_by_id

Para un objeto específico de un tipo de aplicación específico, por ejemplo un proceso de clasificación específico, crea una referencia a un origen de datos.

Tabla 1. create_datasourceRef_by_id

Parámetro	Descripción
appId	Necesario (entero). Identifica la aplicación. Debe ser de esta lista: • 8 = SecurityAssessment • 47 = CustomTables • 51 = Classifier
datasourceId	Necesario (entero). Identifica el origen de datos (de la definición de origen de datos).
objId	Necesario (entero). Identifica una instancia del tipo appID especificado. Por ejemplo, si apID = 51, será el ID de un proceso de clasificación.

Ejemplo

```
grdapi create_datasourceRef_by_id appId=51 datasourceId=20000 objId=2
```

create_datasourceRef_by_name

Para un objeto específico de un tipo de aplicación específico, por ejemplo un proceso de clasificación específico, crea una referencia a un origen de datos.

Tabla 2. create_datasourceRef_by_name

Parámetro	Descripción
application	Necesario. Identifica la aplicación. Debe ser de esta lista: SecurityAssessment CustomTables Classifier
datasourceName	Necesario. Identifica el origen de datos (de la definición de origen de datos).
objName	Necesario. Identifica una instancia del tipo de aplicación especificado. Por ejemplo, si la aplicación es Clasificador, será el nombre de un proceso de clasificación específico.

Ejemplo

```
grdapi  create_datasourceRef_by_name  application=Classifier  datasourceName=swanSybase  objName=”class process1”
```

list_datasourceRef_by_id

Para un objeto específico de un tipo de aplicación específico, por ejemplo un proceso de clasificación específico, lista todos los orígenes de datos a los que se hace referencia.

Tabla 3. list_datasourceRef_by_id

Parámetro	Descripción
appID	Necesario (entero). Identifica la aplicación. Debe ser de esta lista: 8 = SecurityAssessment 47 = CustomTables 51 = Classifier
objID	Necesario. Identifica una instancia del tipo de aplicación especificado. Por ejemplo, si la aplicación es Clasificador, será el ID de un proceso de clasificación específico.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi list_datasourceRef_by_id appId=13 objId=1
```

list_datasourceRef_by_name

Para un objeto específico de un tipo de aplicación específico, por ejemplo un proceso de clasificación específico, lista todos los orígenes de datos a los que se hace referencia.

Tabla 4. list_datasourceRef_by_name

Parámetro	Descripción
application	Necesario. Identifica la aplicación. Debe ser de esta lista: SecurityAssessment CustomTables Classifier
objName	Necesario. Identifica una instancia del tipo de aplicación especificado. Por ejemplo, si la aplicación es Clasificador, será el nombre de un proceso de clasificación específico.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdap list_datasourceRef_by_name application=Classifier  objName="class process1"
```

delete_datasourceRef_by_id

Para un objeto específico de un tipo de aplicación específico, por ejemplo un proceso de clasificación específico, elimina una referencia de origen de datos.

Tabla 5. delete_datasourceRef_by_id

Parámetro	Descripción

Parámetro	Descripción
appId	Necesario (entero). Identifica la aplicación. Debe ser de esta lista: 8 = SecurityAssessment 47 = CustomTables 51 = Classifier
datasourceId	Necesario (entero). Identifica el origen de datos (de la definición de origen de datos).
objId	Necesario (entero). Identifica una instancia del tipo appID especificado. Por ejemplo, si apID = 51, será el ID de un proceso de clasificación.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi delete_datasourceRef_by_id appId=51 datasourceId=2 objId=1
```

delete_datasourceRef_by_name

Para un objeto específico de un tipo de aplicación específico, por ejemplo un proceso de clasificación específico, elimina una referencia de origen de datos.

Tabla 6. delete_datasourceRef_by_name

Parámetro	Descripción
application	Necesario. Identifica la aplicación. Debe ser de esta lista: SecurityAssessment CustomTables Classifier
datasourceName	Necesario. Identifica el origen de datos (de la definición de origen de datos).
objName	Necesario. Identifica una instancia del tipo de aplicación especificado. Por ejemplo, si la aplicación es Clasificador, será el nombre de un proceso de clasificación específico.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi delete_datasourceRef_by_name application=Classifier datasourceName=swanSybase objName="class process1"
```

Tema principal: Referencia de GuardAPI

Funciones de seguridad de usuario de datos de GuardAPI

Utilice estos mandatos de GuardAPI para crear, listar, suprimir y actualizar funciones de seguridad de usuario de datos.

create_user_hierarchy

Añadir una relación entre un usuario y un padre en la jerarquía de seguridad de datos de usuario

Tabla 1. create_user_hierarchy

Parámetro	Descripción

Parámetro	Descripción
userName	Necesario. El nombre del usuario.
parentUserName	Necesario. El nombre del usuario padre.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

grdapi create_user_hierarchy userName=admin parentUserName=accessmgr

Nota: Se produce un error si la inserción es cíclica (un padre informa a un hijo)

list_user_hierarchy_by_parent_user

Listar las relaciones de la jerarquía de seguridad de datos de usuario

Tabla 2. list_user_hierarchy_by_parent_user

Parámetro	Descripción
userName	Necesario. El nombre del usuario.
create	Si se establece (true o false), se generarán o no se generarán sentencias de creación para llamadas a la API create_user_hierarchy. Utilice este parámetro para obtener todos los mandatos necesarios para generar un archivo de proceso por lotes. Este archivo de proceso por lotes se puede utilizar para mover cada emparejamiento de padres e hijos a otro sistema de Guardium.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

grdapi list_user_hierarchy_by_parent_user userName=admin create=true

Nota: Solo lista la relación padre-hijo inmediata. No muestra "nietos"

delete_user_hierarchy_by_entry_id

Suprime una relación de la jerarquía de seguridad de datos de usuario por id de entrada

Tabla 3. delete_user_hierarchy_by_entry_id

Parámetro	Descripción
id	Necesario (entero). Identifica la entrada.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

grdapi delete_user_hierarchy_by_entry_id id=1

Nota: No hay ninguna condición de anomalía si la entrada no existe

delete_user_hierarchy_by_user

Suprime una relación de la jerarquía de seguridad de datos de usuario por usuario

Tabla 4. delete_user_hierarchy_by_user

Parámetro	Descripción
userName	Necesario. El nombre del usuario.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

grdapi delete_user_hierarchy_by_user userName=admin

Nota:

No hay ninguna condición de anomalía si el usuario no existe.

Se llevan a cabo varias supresiones si el usuario tiene varios padres.

create_allowed_db

Crear una relación Usuario-BD

Tabla 5. create_allowed_db

Parámetro	Descripción
userName	Necesario. El nombre del usuario.
serverIp	Necesario. La IP del servidor
instanceName	Necesario. El nombre de instancia
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

grdapi create_allowed_db userName=admin serverIp=192.168.1.1 instanceName=abcd

list_allowed_db_by_user

Listar las asociaciones Usuario-BD por usuario

Tabla 6. list_allowed_db_by_user

Parámetro	Descripción
userName	Necesario. El nombre del usuario.

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

grdapi list_allowed_db_by_user userName=admin

delete_allowed_db_by_entry_id

Suprimir una asociación de Usuario-BD por ID de entrada

Tabla 7. delete_allowed_db_by_entry_id

Parámetro	Descripción
id	Necesario (entero). Identifica la entrada.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

grdapi delete_allowed_db_by_entry_id id=1

delete_allowed_db_by_user

Suprimir una asociación de Usuario-BD por usuario

Tabla 8. delete_allowed_db_by_user

Parámetro	Descripción
userName	Necesario. El nombre del usuario.
serverIp	La IP del servidor.
instanceName	El nombre de instancia. Nota: En los nombres de instancias en "blanco", especifique instanceName=[blank] (y no instanceName=blank)
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

grdapi delete_allowed_db_by_user userName=scott

update_user_db

Aplicar por completo todos los cambios recientes a la correlación de asociaciones Usuario-BD activa

Tabla 9. update_user_db

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

grdapi update_user_db

Nota: En una configuración de gestión Central, este mandato se debe ejecutar en un gestor central.
Tema principal: Referencia de GuardAPI

Funciones de equilibrio de carga de empresa de GuardAPI

Utilice estos mandatos de GuardAPI para ver y establecer los parámetros de equilibrio de carga, ver la correlación de la carga actual y gestionar las asociaciones de S-TAP y los grupos de unidades gestionados.

get_load_balancer_load_map

Ver la correlación de carga actual.

```
grdapi get_load_balancer_load_map
```

get_load_balancer_params

Ver los parámetros de configuración de equilibrio de carga de actual.

```
grdapi get_load_balancer_params
```

set_load_balancer_param

Establecer los parámetros de configuración de equilibrio de carga.

```
grdapi set_load_balancer_param [paramName=value][paramValue=value][paramType=STAP]
```

Consulte la sección Parámetros de configuración de equilibrio de carga de empresa para ver una lista de los parámetros disponibles y los valores permitidos.

Por ejemplo, `grdapi set_load_balancer_params paramName=LOAD_BALANCER_ENABLED paramValue=0 paramType=STAP`

Utilice este formato para la entrada correcta

grdapi set_load_balancer_param --help=true

ID=0

parámetros de función: paramName - Serie - necesario

paramType - Serie - necesario

paramValue - Serie - necesario

Para obtener una lista de valores de constantes para un parámetro, invoque la función con -- get_param_values

assign_load_balancer_groups

Asignar un grupo de unidades gestionadas a una aplicación o un grupo de S-TAP.

```
grdapi assign_load_balancer_groups muGroupName=[value] appGroupName=[value]
```

Parámetro	Valor	Descripción
muGroupName	`nombre de grupo de unidades gestionadas`	Por ejemplo, `muGroupName=mu_group_NA`.
appGroupName	`aplicación o nombre de grupo S-TAP`	Por ejemplo, `appGroupName=app_group_NA`.
ifFailoverGroup	`1 o 0`	Por ejemplo, `isFailoverGroup=0`

unassign_load_balancer_groups

Desasignar un grupo de unidades gestionadas de una aplicación o un grupo de S-TAP.

```
grdapi unassign_load_balancer_groups muGroupName=[value] appGroupName=[value]
```

Parámetro	Valor	Descripción
muGroupName	`nombre de grupo de unidades gestionadas`	Por ejemplo, `muGroupName=mu_group_NA`.
appGroupName	`aplicación o nombre de grupo S-TAP`	Por ejemplo, `appGroupName=app_group_NA`.

Tema principal: Referencia de GuardAPI

Funciones de optimización de titularidades de GuardAPI

Utilice estos mandatos de GuardAPI para habilitar y configurar los informes y orígenes de datos de optimización de titularidades.

enable_entitlement_optimization

Habilita la característica de optimización de titularidades en este recopilador.

```
grdapi enable_entitlement_optimization
```

disable_entitlement_optimization

Inhabilita la característica de optimización de titularidades en este recopilador.

```
grdapi disable_entitlement_optimization
```

add_datasource_to_entitlement_optimization

Añade los datos de este origen a la recopilación de datos de optimización de titularidades y a los separadores individuales, tal como se especifique.

```
grdapi add_datasource_to_entitlement_optimization
```

Parámetro	Valor	Descripción
datasourceName	`datasourceName`	Nombre del origen de datos
isEnabled	uno de los siguientes: `true, false`	El origen de datos está habilitado o inhabilitado, para la optimización de titularidades Valor predeterminado = false
userScope	Uno o varios ID de grupo de usuarios de Guardium, separados por comas. Los grupos deben contener solo usuarios	Opcional. Los resultados de las recomendaciones de titularidades se filtran por este grupo de usuarios. Examinar los resultados de las titularidades: Indica si los usuarios está o no incluidos en este ámbito. No presenta el recuento de actividad de usuarios para los usuarios que están fuera del ámbito. valor predeterminado = NULL
objectScope	Uno o varios ID de grupo de objetos de Guardium, separados por comas. Los grupos deben contener solo objetos.	Opcional. Los resultados de las recomendaciones de titularidades se filtran por este grupo de objetos. valor predeterminado = NULL
extractActivity	uno de los siguientes: `true, false`	Habilita o inhabilita la extracción de la actividad de orígenes de datos. Debe ser true para Examinar titularidades y para Probabilidad. Valor predeterminado = false
extractEntitlement	uno de los siguientes: `true, false`	Habilita o inhabilita la extracción de datos de titularidades. Debe ser true para Novedades, Usuarios y roles, Recomendaciones y Examinar titularidades Valor predeterminado = false
generateRoleClusters	uno de los siguientes: `true, false`	Habilita o inhabilita la extracción de la agrupación en clúster de roles por comportamiento, desde el origen de datos, que se utiliza en el separador **Probabilidad**. Debe ser true para Probabilidad. Valor predeterminado = false
generateNews	uno de los siguientes: `true, false`	La actividad de este origen de datos se incluye en el separador **Novedades**. Valor predeterminado = false
generateRecommendations	uno de los siguientes: `true, false`	La actividad de este origen de datos se incluye en el separador **Recomendaciones**. Valor predeterminado = false
filterTempObjects	uno de los siguientes: `true, false`	Para uso futuro. Los objetos temporales se filtran a partir de los datos recopilados del origen de datos. Valor predeterminado = true
filterIgnoreVerbs	uno de los siguientes: `true, false`	Para uso futuro. Los verbos omitidos se filtran a partir de los datos recopilados del origen de datos. Valor predeterminado = true

remove_datasource_from_entitlement_optimization

Elimina todos los datos de este origen de la recopilación de datos de optimización de titularidades.

```
remove_datasource_from_entitlement_optimization
```

set_entitlement_datasource_parameter

Modifica los parámetros para el origen de datos que ya está habilitado para la optimización de titularidades. Utiliza los mismos parámetros que add_datasource_to_entitlement_optimization.

```
grdapi set_entitlement_datasource_parameter
```

get_entitlement_datasource_parameter

Muestra los valores de los parámetros para cada origen de datos en este recopilador.

```
grdapi get_entitlement_datasource_parameter
```

Ejemplo:

```
La optimización de titularidades está habilitada
==================================
Datasource: SCALE-DB16
==================================
isEnabled: true
userScope:
objectScope:
extractActivity: true
extractEntitlement: true
generateRoleClusters: true
generateNews: true
generateRecommendations: true
filterTempObjects: true
filterIgnoreVerbs: true
==================================
Datasource: on12scal
==================================
isEnabled: true
userScope:
objectScope:
extractActivity: true
extractEntitlement: true
generateRoleClusters: true
generateNews: true
generateRecommendations: true
filterTempObjects: true
filterIgnoreVerbs: true
```

Tema principal: Referencia de GuardAPI

Funciones de canal de información externo de GuardAPI

Utilice estas funciones GuardAPI para crear correlaciones para canales de información externos.

create_ef_mapping

Esta función crea una correlación y llena las tablas basándose en el nombre del informe especificado en el parámetro *reportName*. Cada correlación tiene un nombre almacenado en EF_MAP_TYPE_HDR.EF_TYPE_DESC, y ese nombre será idéntico al valor de *reportName*. El nombre de tabla de destino también se basará en el parámetro *reportName*, con signos subrayado añadidos entre las palabras. Por ejemplo, "My Report" se convierte en MY_REPORT.

Tabla 1.

Parámetro	Descripción
reportName	Nombre del informe que se ha de utilizar para la correlación de canales de información externos. Este parámetro también determina el nombre de la correlación y el nombre de la tabla de destino.

modify_ef_mapping

Algunas veces, los nombres generados por create_ef_mapping no son adecuados para una base de datos concreta, y se puede utilizar modify_ef_mapping para adaptar los nombres a los requisitos de la base de datos. Sólo se pueden modificar las correlaciones con ID >= 20000, para proteger las correlaciones predefinidas de Guardium.

Tabla 2.

Parámetro	Descripción
reportName	Nombre de la correlación que se ha de modificar.
modifyObj	Especifica el objeto de base de datos a modificar, *tabla* o *columna*. Los valores existentes se pueden recuperar utilizando la función list_ef_mapping.
oldName	Especifica el nombre de tabla antiguo que se va a eliminar.
newName	Especifica el nombre de tabla nuevo que se va a eliminar.

delete_ef_mapping

Esta función le permite suprimir correlaciones existentes. Sólo se pueden suprimir las correlaciones con ID >= 20000, para proteger las correlaciones predefinidas de Guardium.

Tabla 3.

Parámetro	Descripción
reportName	Nombre de la correlación que se ha de suprimir.

list_ef_mapping

Si se ejecuta sin ningún parámetro, esta función devuelve una lista de todas las correlaciones creadas por el cliente. Si se ejecuta con el parámetro *reportName*, esta función devuelve detalles de la correlación especificada, por ejemplo, los nombres de tabla y columna utilizados por el canal de información externo.

Tabla 4.

Parámetro	Descripción
reportName	Opcional. Nombre de la correlación para la que se devuelven los detalles.

Tema principal: Referencia de GuardAPI

Funciones de FAM (File Activity Monitor) de GuardAPI

Utilice los siguientes mandatos de GuardAPI para habilitar e inhabilitar la actividad del supervisor de actividad de archivos, configurar la actividad del panel de investigación de archivos, la planificación de las extracciones de titularidad y obtener información acerca del supervisor de actividad de archivos.

Utilice el mandato GuardAPI, grdapi create_policy, para crear una política de FAM. Una vez creada la política, utilice los mandatos de GuardAPI específicos de FAM.

Por ejemplo:

grdapi create_policy ruleSetDesc='TEST'

grdapi create_fam_rule policyName='TEST' ruleName=r-test-sles11 actionName="Log As Violation and Audit" serverHost="9.70.144.98:FAM" filePath="/famtest/*"

Para obtener instrucciones sobre cómo utilizar los mandatos de GuardAPI, consulte la sección Referencia de GuardAPI.

enable_fam_crawler

Establece el sistema Guardium para procesar los resultados del rastreador y los datos de actividad de archivos. Los resultados se añadirán automáticamente a los archivos de índice de búsqueda rápida. Utilice los parámetros para planificar la actividad de búsqueda rápida, las extracciones de titularidad y el llenado de grupos remotos.

Nota: El panel de control de investigación también se debe habilitar con el mandato grdapi enable_quick_search schedule_interval=1.

Tabla 1. enable_fam_crawler

Parámetro	Descripción
extraction_start	Fecha/hora inicial en la que se extraen los datos en la búsqueda rápida de archivos. Está limitado a 2 días en el pasado. El valor predeterminado es la hora actual. Si la unidad se establece en HOUR, se redondea a una hora. Si se establece en DAY, se redondea a un día.
schedule_start	El valor predeterminado es la hora actual.
activity_schedule_interval	Necesario. Este parámetro establece el intervalo de planificación de las actividades. El intervalo recomendado es 2 con la unidad establecida en MINUTE.
activity_schedule_units	Necesario. Este parámetro establece la unidad de la unidad de actividad. Los valores son: MINUTE u HOUR. La unidad recomendada es MINUTE.
entitlement_schedule_interval	Necesario. Este parámetro establece el intervalo de planificación de titularidad. El intervalo recomendado es 1, con la unidad establecida en DAY.
entitlement_schedule_units	Necesario. Este parámetro establece la unidad de la planificación de titularidad. Los valores posibles son MINUTE, HOUR y DAY. La unidad recomendada es DAY.

Ejemplo

```
grdapi enable_fam_crawler extraction_start=< > schedule_start=< >
 activity_schedule_interval=2 activity_schedule_units=MINUTE
entitlement_schedule_interval=10 entitlement_schedule_units=MINUTE
```

disable_fam_crawler

Inhabilita el supervisor de actividades de archivos. Se eliminan las extracciones de titularidad y la actividad de búsqueda rápida de archivos. Esta función también inhabilita el llenado del grupo.

Ejemplo

```
grdapi disable_fam_crawler
```

get_fam_crawler_info

Muestra el estado del supervisor de actividades de archivo. Si se habilita, el mandato muestra los valores para la planificación de la actividad de búsqueda rápida de archivos y la extracción de archivos.

```
El rastreador FAM (lado del servidor) está inhabilitado.
```

```
El rastreador FAM (lado del servidor) está inhabilitado. Titularidad (1 DAY) Actividad (2 MINUTE)
```

Ejemplo

```
grdapi get_fam_crawler_info
```

list_policy_fam_rule

Lista todas las reglas de una política de FAM.

Parámetro	Descripción
policyName	Necesario. Serie. Nombre de política
ruleName	Opcional. Serie. Si no se proporciona ningún valor para ruleName, se mostrarán todas las reglas de política con detalles. Si se proporciona un valor para ruleName, se listarán los detalles de dicha regla.

create_fam_rule

Crea una regla de FAM nueva.

Parámetro	Descripción
policyName	Necesario. Serie. Nombre de la política.
ruleName	Necesario. Serie. Nombre de la regla.
filePath	Serie. La vía de acceso que se va a supervisar. Se debe especificar filePath o filePathGroup.
notfilePath	Serie. Debe ser yes o no. Yes significa aplicar esta regla a todos los archivos, excepto los que están en la vía de acceso especificada.
filePathGroup	Serie. Grupo de vías de acceso. Se debe especificar filePath o filePathGroup.
includeSubDirectory	Serie. Debe ser yes o no. Yes significa incluir los archivos de todos los subdirectorios.
removableMedia	Serie. Debe ser yes o no.
osUser	Serie. Nombre de usuario de SO
osUserGroup	Serie. Grupo de usuarios de SO.
notOSUser	Serie. Debe ser yes o no. Yes significa utilizar todos los usuarios, excepto el osUser especificado.
serverHost	Serie. Nombre de host.
serverHostGroup	Serie. Grupo de nombres de host.
command	Serie. El nombre de mandato que se va a incluir en la regla, uno de los siguientes • DELETE • EXECUTE • FILEOP • READ • WRITE
commandGroup	Serie. Grupo de mandatos.
notCommand	Serie. Debe ser yes o no. Yes significa utilizar todos los mandatos, excepto el mandato especificado.
actionName	Serie. Necesario. El nombre de la acción de FAM.
messageTemplate	Serie. Nombre de la plantilla de mensajes.
notificationType	Serie. Tipo de notificación. Uno de los siguientes: • MAIL • SNMP • CUSTOM • SYSLOG
userLoginName	Serie. Nombre de inicio de sesión de usuario.
classDestination	Serie. Nombre de la clase personalizada que se ha de invocar.

policy_fam_rule_delete

Suprime una regla de una política FAM.

Parámetro	Descripción
policyName	Necesario. Serie. Nombre de política
ruleName	Necesario. Serie. Nombre de la regla que se ha de suprimir.

add_action_to_fam_rule

Añade una acción a una regla FAM existente.

Parámetro	Descripción
actionName	Serie. Necesario. El nombre de la acción de FAM.
alertReceiver	AlertReceiver es cualquier usuario del dispositivo como, por ejemplo, admin.
command	Serie. El nombre de mandato que se va a incluir en la regla. Uno de los siguientes: • DELETE • EXECUTE

	• FILEOP • READ • WRITE
messageTemplate	Serie. Nombre de la plantilla de mensajes.
notificationType	Serie. Tipo de notificación, uno de los siguientes: • MAIL • SNMP • CUSTOM • SYSLOG
policyName	Necesario. Serie. Nombre de política válido.
ruleName	Necesario. Serie. Nombre de la regla que se ha de actualizar.

Tema principal: Referencia de GuardAPI

Funciones GIM de GuardAPI

Utilice estos mandatos de CLI para listar, actualizar, asignar, eliminar y cancelar funciones GIM.

gim_list_registered_clients

Lista todos los clientes registrados.

Tabla 1. gim_list_registered_clients

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi gim_list_registered_clients
```

gim_list_client_params

Lista todos los parámetros (módulo) asignados a un cliente específico.

Tabla 2. gim_list_client_params

Parámetro	Descripción
clientIP	Necesario - Dirección IP del cliente
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi gim_list_client_params clientIP=192.168.12.210
```

gim_update_client_params

Actualiza los parámetros de un único módulo en un cliente específico.

Tabla 3. gim_update_client_params

Parámetro	Descripción
clientIP	Necesario. IP del cliente de destino

Parámetro	Descripción
paramName	Necesario. El nombre del parámetro
paramValue	Necesario. El valor del parámetro
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi gim_update_client_params clientIP=192.168.1.100 paramName=STAP_TAP_IP paramValue=192.168.1.100
```

gim_list_client_modules

Lista todos los módulos asignados a un cliente específico y su estado

Tabla 4. gim_list_client_modules

Parámetro	Descripción
clientIP	Necesario - Dirección IP del cliente
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi gim_list_client_modules clientIP=192.168.2.210
```

gim_load_package

Carga todos los módulos en el 'filename'.

Nota: Este mandato carga un archivo que reside en el sistema local, por lo tanto el procedimiento (cmd='fileserver') de cargar un archivo en el dispositivo Guardium o CM debe realizarse antes de ejecutar este mandato.

Tabla 5. gim_load_package

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi gim_load_package  filename=*.gim
```

Nota: Se puede utilizar el carácter comodín "*" en el nombre de archivo.

gim_assign_bundle_or_module_to_client_by_version

Asigna un paquete o módulo a un cliente.

Tabla 6. gim_assign_bundle_or_module_to_client_by_version

Parámetro	Descripción
clientIP	Necesario - Dirección IP del cliente
module	Necesario - Módulo
moduleVersion	Necesario - Versión del módulo
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi gim_assign_bundle_or_module_to_client_by_version clientIP=192.168.1.100  module=BUNDLE-STAP moduleVersion="8.0_r1234_1"
```

gim_schedule_install

Planifica la instalación de todos los paquetes o módulos asignados a un cliente y que todavía no se han instalado, por ejemplo, PENDING. Si el parámetro module es específico, solo se planifica el módulo solicitado.

Tabla 7. gim_schedule_install

Parámetro	Descripción
clientIP	Necesario - Dirección IP del cliente
module	Opcional - Módulo. Si no se especifica el módulo en el mandato, se planifica la instalación de todos los módulos de la IP de cliente especificada.
date	Necesario - Fecha. Formato: 'now' o 'aaaa-MM-dd HH:mm'
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi gim_schedule_install clientIP=192.168.1.100 module=BUNDLE-STAP  date="2008-07-02 14:50"
```

```
grdapi gim_schedule_install clientIP=192.168.1.100 date="2008-07-02 14:50"
```

Nota: Se puede utilizar una fecha del pasado para que se ejecute algún proceso de forma inmediata.

gim_list_client_status

Muestra el estado de la operación ejecutada más recientemente para un cliente específico.

Tabla 8. gim_list_client_status

Parámetro	Descripción
clientIP	Necesario - Dirección IP del cliente
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi gim_list_client_status clientIP=192.168.1.100
```

gim_uninstall_module

Desinstala un módulo o paquete en un cliente específico.

Tabla 9. gim_uninstall_module

Parámetro	Descripción
clientIP	Necesario - Dirección IP del cliente
module	Necesario - Módulo.
date	Necesario - Fecha. Formato: 'now' o 'aaaa-MM-dd HH:mm'
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi gim_uninstall_module clientIP=192.168.1.100 module=BUNDLE-STAP
```

gim_cancel_install

Cancela la instalación de un paquete o módulo en un cliente específico. Solo se puede cancelar la instalación si el módulo o paquete todavía no está en el proceso de ser instalado por un cliente (STATE=IP o IP-PR)

Tabla 10. gim_cancel_install

Parámetro	Descripción
clientIP	Necesario - Dirección IP del cliente
module	Necesario - Módulo.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi gim_cancel_install clientIP=192.168.1.100 module=BUNDLE-STAP
```

gim_list_bundles

Lista todos los paquetes disponibles. Un paquete es un grupo de módulos que se puede instalar en un cliente.

Tabla 11. gim_list_bundles

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi gim_list_bundles
```

gim_list_mandatory_params

Lista los parámetros obligatorios para un módulo individual.

Tabla 12. gim_list_mandatory_params

Parámetro	Descripción
module	El nombre del módulo GIM para el que se han de mostrar los parámetros obligatorios.
version	La versión del módulo GIM para el que se han de mostrar los parámetros obligatorios.

Ejemplo

```
grdapi gim_list_mandatory_params module=nombre version=número
```

gim_assign_latest_bundle_or module_to_client

Asigna el paquete o módulo disponible más reciente (la versión más alta) de un cliente específico.

Tabla 13. gim_assign_latest_bundle_or module_to_client

Parámetro	Descripción
clientIP	Necesario - Dirección IP del cliente
module	Necesario - Módulo.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi gim_assign_latest_bundle_or_module_to_client clientIP=192.168.1.100  module=BUNDLE_STAP
```

gim_schedule_uninstall

Planifica la desinstalación de todos los paquetes o módulos asignados a un cliente y que todavía no se han desinstalado, por ejemplo, PENDING. Si el parámetro 'module' es específico, solo se planifica el módulo solicitado.

Tabla 14. gim_schedule_install

Parámetro	Descripción
clientIP	Necesario - Dirección IP del cliente
module	Opcional - Módulo. Si no se especifica el módulo en el mandato, se planifica la instalación de todos los módulos de la IP de cliente especificada.
date	Necesario - Fecha. Formato: 'now' o 'aaaa-MM-dd HH:mm'
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi gim_schedule_uninstall clientIP=192.168.1.100 module=BUNDLE-STAP  date=”2008-07-02 14:50”   grdapi gim_schedule_uninstall clientIP=192.168.1.100 date=”2008-07-02 14:50”
```

gim_cancel_uninstall

Cancela la desinstalación de un paquete o módulo en un cliente específico. Solo se puede cancelar la desinstalación si el módulo o paquete todavía no está en el proceso de ser desinstalado por un cliente (STATE=IP o IP-PR)

Tabla 15. gim_cancel_uninstall

Parámetro	Descripción
clientIP	Necesario - Dirección IP del cliente
module	Necesario - Módulo.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi gim_cancel_uninstall clientIP=192.168.1.100 module=BUNDLE-STAP
```

gim_remove_bundle

El mandato suprime bundlePackageName de la base de datos y también del sistema de archivos, del directorio /var/log/guard/gim_packages y también de /var/gim_dist_packages si el sistema Guardium es un gestor central.

parámetros (necesarios):

bundlePackageName

El valor del parámetro toma el nombre del paquete, según se especifica en la salida de gim_list_unused_bundles. El mandato solo se ejecuta correctamente si:

2.1 El valor de bundlePackageName hace referencia a un BUNDLE

2.2 El valor de bundlePackageName no está asignado a ningún cliente

2.3 El valor de bundlePackageName existe

2.4 Solo hay un único modo de que un paquete haga referencia al valor de bundlePackageName

TODAS las condiciones (2.1 a 2.4) deben cumplirse para suprimir un paquete de la base de datos o el sistema de archivos. De lo contrario, se genera un error.

Ejemplo

```
grdapi gim_remove_bundle  bundlePackageName= bundlePackageName
```

gim_unassign_client_module

Desasigna un paquete o módulo de un cliente. A diferencia de 'gim_remove_module', este mandato desenlaza la conexión entre un módulo y un cliente específico en el dispositivo Guardium o CM. Este mandato NO desinstalará ni eliminará el módulo de la máquina de servidor de BD real. Solo se ha de utilizar si se producen problemas de sincronización entre la información del servidor de BD, por ejemplo el cliente, y la información del dispositivo Guardium o relacionada con el estado actual de los módulos.

Tabla 16. gim_unassign_client_module

Parámetro	Descripción
clientIP	Necesario - Dirección IP del cliente
module	Opcional - Módulo. Si no se especifica el módulo en el mandato, se planifica la instalación de todos los módulos de la IP de cliente especificada.
date	Necesario - Fecha. Formato: 'now' o 'aaaa-MM-dd HH:mm'
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi gim_unassign_client_module clientIP=192.168.1.100  module=STAP
```

gim_get_purge_list

Listar todos los paquetes de software antiguos (archivo GIM) que se han cargado anteriormente al dispositivo Guardium o CM.

Tabla 17. gim_get_purge_list

Parámetro	Descripción
olderThan	Necesario - Número de días. Se depuran los archivos más antiguos que el número de días especificado. El valor válido es número igual o mayor que 0.
excludeLatest	Opcional - true o false (el valor predeterminado es true). true – Evitar la depuración de la última versión por SO por módulo. true – Depurar la última versión por SO por módulo.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi gim_get_purge_list olderThan=30 excludeLatest=true
```

gim_purge

Eliminar todos los paquetes de software antiguos (archivo GIM) que se han cargado anteriormente al dispositivo Guardium o CM.

Tabla 18. gim_purge

Parámetro	Descripción
olderThan	Necesario - Número de días. Se depuran los archivos más antiguos que el número de días especificado. El valor válido es número igual o mayor que 0.
excludeLatest	Opcional - true o false (el valor predeterminado es true). true – Evitar la depuración de la última versión por SO por módulo. true – Depurar la última versión por SO por módulo.
filename	Opcional - Un archivo específico que ha de eliminar. Si el archivo especificado es un paquete, por ejemplo comienza por 'guard-bundle', se eliminará el contenido de este paquete.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi gim_purge olderThan=30
```

Nota:

En el mandato se puede especificar el parámetro 'filename' o el parámetro olderThan y/o excludeLatest.

La depuración de GIM no depura los archivos planificados para su instalación en este momento.

La depuración de GIM no permite que se elimine ningún archivo, por ejemplo el parámetro filename, que incluya el carácter '/'.

gim_get_available_modules

Listar los módulos o paquetes disponibles para instalar en un servidor específico.

Tabla 19. gim_get_available_modules

Parámetro	Descripción
clientIP	Necesario - Dirección IP del cliente

Ejemplo

```
grdapi gim_get_available_modules clientIP=192.168.1.100
```

gim_get_client_last_event

Listar la operación ejecutada más recientemente para un cliente específico.

gim_get_client_last_event es un mandato GrdAPI con funciones limitadas. Lo único que hace es mostrar el último suceso ocurrido durante el intento de instalación más reciente. Por ejemplo si durante la última instalación de S-TAP se han producido errores, se muestran si se ejecuta este mandato grdapi. No obstante, si arregla manualmente el problema directamente en el servidor de base de datos, este mandato grdapi continuará mostrando el mismo mensaje de error original, a pesar de que ahora se esté ejecutando S-TAP. Este mandato no se debe utilizar para evaluar el estado de S-TAP después de realizar arreglos manuales en el servidor de bases de datos.

Tabla 20. gim_get_client_last_event

Parámetro	Descripción
clientIP	Necesario - Dirección IP del cliente

Ejemplo

grdapi gim_get_client_last_event clientIP=192.168.1.100

grdapi gim_get_client_last_event clientIP=winx64

grdapi gim_get_client_last_event clientIP=9.70.144.73

gim_get_modules_running_status

Listar los módulos o paquetes que se están ejecutando actualmente en un servidor específico.

Tabla 21. gim_get_modules_running_status

Parámetro	Descripción
clientIP	Necesario - Dirección IP del cliente
process	nombre del proceso
status	ON u OFF
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi gim_get_modules_running_status clientIP=192.168.1.100 process= status=
```

gim_list_unused_bundles

El mandato devuelve una lista de paquetes no utilizados (no instalados en ningún servidor de base de datos) y módulos de Windows individuales que se puede cargar, por ejemplo, Windows CAS, Windows FAM.

parámetros (necesarios):

includeLatest (valores válidos 0/1)

Si se establece en el valor 1, la lista de paquetes no utilizados devuelta incluye el último paquete no utilizado.

Ejemplo

```
grdapi gim_list_unused_bundles includeLatest=1
```

gim_reset_client

Desasociar módulos del cliente seleccionado.

Tabla 22. gim_reset_client

Parámetro	Descripción
clientIP	Necesario - Dirección IP del cliente

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi gim_reset_client clientIP=192.168.1.100
```

gim_set_diagnostics

Establecer la recopilación de diagnósticos con GIM.

Tabla 23. gim_set_diagnostics

Parámetro	Descripción
clientIP	Necesario - Dirección IP del cliente
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi gim_set diagnostics clientIP=192.168.1.100
```

gim_set_global_param

Establecer parámetros globales en GIM.

Tabla 24. gim_set_global_param

Parámetro	Descripción
clientIP	Necesario - Dirección IP del cliente
paramName	Necesario - Nombre del parámetro en la función de API que se va a correlacionar
paramValue	Necesario - Valor del parámetro en la función de API que se va a correlacionar
sqlguardip	Opcional - Dirección IP/nombre de host del recopilador al que se conectará este agente de GIM.
ca_file	Opcional - Vía de acceso del nombre de archivo completo del archivo PEM de la entidad emisora de certificados.
key_file	Opcional - Vía de acceso del nombre de archivo completo del archivo PEM de clave privada.
cert_file	Opcional - Vía de acceso del nombre de archivo completo del archivo PEM de certificado.
gim_listener_default_port	Opcional - Establecer un puerto diferente para el modo de servidor del agente GIM.
gim_listener_default_shared_secret	Opcional - Establecer un secreto compartido para verificar los recopiladores que están enviando solicitudes al agente GIM en modalidad de servidor nuevo.
no_listener	Opcional - Inhabilitar el agente de GIM en modalidad de servidor.

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi gim_set_global_param clientIP=192.168.1.100 paramName=gim_listener_default_port paramValue=8445
```

gim_remote_activation

Conecta la dirección IP del recopilador a un agente GIM en modalidad de servidor o a un grupo de agentes GIM.

Tabla 25. gim_remote_activation

Parámetro	Descripción
targetGroup	Opcional - El nombre de grupo de todos los servidores de bases de datos a los que se conecta el recopilador. No se puede especificar con el parámetro targetHost.
sharedSecret	Opcional - El secreto compartido que se ha configurado durante la instalación.
targetPort	Opcional - La modalidad de servidor de puerto del agente GIM.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi gim_remote_activation targetGroup=<someGroup> sharedSecret=<password> targetPort=8445
```

Tema principal: Referencia de GuardAPI

Funciones de grupo de GuardAPI

Utilice estos mandatos GuardAPI para crear, listar, suprimir y actualizar funciones de grupos de orígenes de datos.

Nota: En un entorno de gestión Central, todos los grupos se definen en el Gestor central y se envían a las unidades gestionadas de forma planificada.

Funciones de grupo

create_group

list_group_by_id

list_group_by_desc

delete_group_by_id

delete_group_by_desc

update_group_by_id

update_group_by_desc

flatten_hierarchical_groups

Funciones de los miembros

create_member_to_group_by_id

create_member_to_group_by_desc

list_group_members_by_id

list_group_members_by_desc

delete_member_from_group_by_id

delete_member_from_group_by_desc

create_group

create_group

Crear una definición de grupo.

Tabla 1. create_group

Parámetro	Descripción
desc	Necesario. Escriba una descripción exclusiva del nuevo grupo.
type	Necesario. Debe ser uno de los siguientes: Número de valor de suceso de aplicación Serie de valor de suceso de aplicación Tipo de valor de suceso de aplicación Nombre de elemento de aplicación Módulo de aplicación ID de sistema de aplicaciones Código de transacción de aplicación USUARIO DE APLICACIONES Tipo de tarea de auditoría Nombre de host del cliente IP de cliente IP de cliente/Usuario de BD IP de cliente/Aplic. de origen/Usuario de BD IP Cliente/Aplic. Orig./Usuarios BD/IP Servidor/Nombres servicio Dirección MAC del cliente SO de cliente MANDATOS Pruebas predefinidas de CVE Nombre de base de datos Códigos de error de BD PROTOCOLO DE BD VERSIÓN DE PROTOCOLO DE BD Rol de BD Usuario de BD/Objeto/Privilegio Ver./Parches de BD TIPO DE EXCEPCIÓN CAMPOS Permisos de archivos ID global Categorías de auditoría de Guardium Rol de Guardium Usuarios de Guardium Código de inicio de sesión correcto PROTOCOLO DE RED Objeto/Mandato Objeto/Campo

Parámetro	Descripción
	OBJETOS Tipo de operación Usuario de SO PUERTO Objetos cualificados Registros afectados ESQUEMA PROFUNDIDAD DE SENTENCIA Descripción del servidor Nombre de host del servidor IP de servidor IP de servidor/Usuario de BD IP de servidor/Puerto de servidor IP de servidor/Nombre de svc./Usuario de BD SO de servidor TIPO DE SERVIDOR Nombre de servicio PROGRAMA FUENTE Pruebas predefinidas basadas en SQL Perfil de TeraData/Usuario de BD TTL USUARIOS Excepción de pruebas de VA DÍASEM AÑO
appid	Necesario. Identifica la aplicación para el grupo. Debe ser uno de los valores siguientes: Público Creador de procesos de auditoría Creador de línea base Atención: El Creador de líneas base y la funcionalidad relacionada con el mismo está en desuso desde Guardium V10.1.4. Clasificador Grupos de zOS de DB2 Seguridad exprés Grupos de zOS de IMS Creador de políticas Creador de asesoramientos de seguridad
subtype	Opcional. Se utiliza un subtipo para recopilar varios grupos del mismo tipo de grupo, donde la pertenencia de cada grupo es exclusiva. Por ejemplo, suponga que tiene servidores de bases de datos ubicados en tres centros de datos y que desea agrupar los servidores por ubicación. Debe definir un grupo separado de servidores de bases de datos para cada ubicación, y definir los tres grupos con el mismo subtipo (el centro de datos, por ejemplo).
category	Opcional. Una categoría es una etiqueta opcional que se utiliza para agrupar infracciones de políticas y grupos para crear informes.
classification	Opcional. Una clasificación es una etiqueta opcional que se utiliza para agrupar infracciones de políticas y grupos para crear informes.

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplos (siga exactamente las mayúsculas y minúsculas cuando se indiquen)

```
grdapi create_group desc=agroup type=OBJECTS  appid=Public owner=admin
```

```
grdapi create_group appid=Access_policy owner=admin  type="OBJECTS"  desc=groupName1
```

list_group_by_id

Muestra las propiedades de un grupo específico.

Tabla 2. list_group_by_id

Parámetro	Descripción
id	Necesario (entero). Identifica el grupo.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi list_group_by_id id=100003
```

list_group_by_desc

Muestra las propiedades de un grupo específico.

Tabla 3. list_group_by_desc

Parámetro	Descripción
desc	Necesario. El nombre del grupo que se va a visualizar.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi list_group_by_desc desc=agroup
```

delete_group_by_id

Tabla 4. delete_group_by_id

Parámetro	Descripción
id	Necesario (entero). Identifica el grupo.

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi delete_group_by_id id=100005
```

delete_group_by_desc

Tabla 5. delete_group_by_desc

Parámetro	Descripción
desc	Necesario. El nombre del grupo que se va a eliminar.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi delete_group_by_desc desc=agroup
```

update_group_by_id

Actualizar las propiedades del grupo.

Tabla 6. update_group_by_id

Parámetro	Descripción
id	Necesario (entero). Identifica el grupo que se va actualizar.
newDesc	Opcional. Escriba una descripción exclusiva del nuevo grupo.
subtype	Opcional. Se utiliza un subtipo para recopilar varios grupos del mismo tipo de grupo, donde la pertenencia de cada grupo es exclusiva. Por ejemplo, suponga que tiene servidores de bases de datos ubicados en tres centros de datos y que desea agrupar los servidores por ubicación. Debe definir un grupo separado de servidores de bases de datos para cada ubicación, y definir los tres grupos con el mismo subtipo (el centro de datos, por ejemplo).
category	Opcional. Una categoría es una etiqueta opcional que se utiliza para agrupar infracciones de políticas y grupos para crear informes.
classification	Opcional. Una clasificación es una etiqueta opcional que se utiliza para agrupar infracciones de políticas y grupos para crear informes.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi update_group_by_id id=100002 newDesc=beegroup subtype=bee category=be classification=bea
```

update_group_by_desc

Actualizar las propiedades del grupo.

Tabla 7. update_group_by_desc

Parámetro	Descripción
desc	Necesario. El nombre del grupo que se va a actualizar.
newDesc	Opcional. Escriba una descripción exclusiva del grupo.
subtype	Opcional. Se utiliza un subtipo para recopilar varios grupos del mismo tipo de grupo, donde la pertenencia de cada grupo es exclusiva. Por ejemplo, suponga que tiene servidores de bases de datos ubicados en tres centros de datos y que desea agrupar los servidores por ubicación. Debe definir un grupo separado de servidores de bases de datos para cada ubicación, y definir los tres grupos con el mismo subtipo (el centro de datos, por ejemplo).
category	Opcional. Una categoría es una etiqueta opcional que se utiliza para agrupar infracciones de políticas y grupos para crear informes.
classification	Opcional. Una clasificación es una etiqueta opcional que se utiliza para agrupar infracciones de políticas y grupos para crear informes.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi update_group_by_desc desc=beegroup newDesc=beegroupee category=bebebe classification=bebebebe
```

flatten_hierarchical_groups

Actualizar TODOS los grupos jerárquicos que existen en el creador de grupos.

Tabla 8. flatten_hierarchical_groups

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi flatten_hierarchical_groups
```

create_member_to_group_by_id

Añadir un miembro a un grupo especificado mediante el ID de grupo.

Tabla 9. create_member_to_group_by_id

Parámetro	Descripción
id	Necesario (entero). Identifica el grupo al que se ha de añadir el miembro.
member	Necesario. El nombre del nuevo miembro, que debe ser exclusivo en el grupo.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi create_member_to_group_by_id  id=100005 member=turkey
```

create_member_to_group_by_desc

Añadir un miembro al grupo nombrado.

Tabla 10. create_member_to_group_by_desc

Parámetro	Descripción
desc	Necesario. El nombre del grupo al que se ha de añadir el miembro.
member	Necesario. El nombre del nuevo miembro, que debe ser exclusivo en el grupo.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi create_member_to_group_by_desc  desc=bgroup  member=turkey
```

Utilice estos mandatos para añadir miembros al grupo:

```
grdapi create_member_to_group_by_desc desc=groupName1 member=member_1
grdapi create_member_to_group_by_desc desc=groupName1 member=member_2
grdapi create_member_to_group_by_desc desc=groupName1 member=member_3
grdapi create_member_to_group_by_desc desc=groupName1 member=member_4
grdapi create_member_to_group_by_desc desc=groupName1 member=member_5
```

Mandatos de GuardAPI de grupo adicionales

create_hierarchical_member_to_group_by_desc

delete_hierarchical_member_from_group_by_desc

parámetros de función:

desc - Serie - necesario

member - Serie - necesario

list_group members_by_id

Listar los miembros del grupo especificado.

Tabla 11. list_group members_by_id

Parámetro	Descripción
id	Necesario (entero). Identifica el grupo cuyos miembros se han de listar.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi list_group_members_by_id  id=100001
```

list_group_members_by_desc

Listar los miembros del grupo especificado.

Tabla 12. list_group_members_by_desc

Parámetro	Descripción
desc	Necesario. El nombre del grupo cuyos miembros se han de listar.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi list_group_members_by_desc  desc=bgroup
```

delete_member_from_group_by_id

Eliminar un miembro de un grupo especificado.

Tabla 13. delete_member_from_group_by_id

Parámetro	Descripción
id	Necesario (entero). Identifica el grupo del que se ha de eliminar el miembro.
member	Necesario. El nombre del miembro que se va a eliminar.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi delete_member_to_group_by_id  id=100005 member=turkey
```

delete_member_from_group_by_desc

Eliminar un miembro de un grupo especificado.

Tabla 14. delete_member_from_group_by_desc

Parámetro	Descripción
desc	Necesario. El nombre del grupo del que se ha de eliminar el miembro.
member	Necesario. El nombre del miembro que se va a eliminar.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi delete_member_from_group_by_desc desc=bgroup member=boston
```

Tema principal: Referencia de GuardAPI

Generación de entrada de GuardAPI

La generación de entrada de GuardAPI permite al usuario tomar la salida de un informe de Guardium y pasarla como entrada a otra entidad de Guardium. Lo permite a los usuarios utilizar llamadas preparadas para invocar las funciones de API.

Generar entrada para llamadas de Guard API

Se puede invocar la generación de llamadas de Guard API a partir de informes de una de las dos maneras siguientes: Desde una sola fila de un informe o desde varias filas basadas en un informe (lo que se ve en la pantalla). Consulte el tema sobre cómo generar llamadas a la API desde informes, para obtener un ejemplo.

Cuando se visualiza un informe:

Para una sola fila:

1. Si pulsa dos veces una fila para detallar más, se muestra una opción Invocar. Pulse la opción Invocar para ver una lista de las API correlacionadas con este informe.

Para varias filas

1. Pulse el icono Invocar (en la línea de estado del informe) para ver una lista de las API correlacionadas con este informe.

   Continúe realizando los pasos para una o varias filas.

2. Pulse la API que desee invocar; abriendo el formulario de llamada a API del informe y la función de API invocada. Invocar una llamada de API desde un informe para varias filas genera un formulario de llamada de API que visualiza y permite la edición de todos los registros que se muestran en la pantalla (en función del tamaño de captación) hasta un máximo de 20 registros.
3. Rellene los parámetros necesarios y algunos de los parámetros no necesarios para la llamada de API seleccionada. Muchos de los parámetros se rellenan previamente desde el informe, pero se pueden cambiar para crear una llamada de API exclusiva. Para obtener ayuda específica para rellenar los parámetros necesarios o no necesarios, consulte las llamadas de función de API individuales en la guía de consulta de GuardAPI.
   Para varias filas, utilice el conjunto de parámetros para la API (con un botón para cada parámetro) para especificar un valor para un parámetro y, a continuación, pulse el botón de flecha abajo para rellenar dicho parámetro para todos los registros. Asimismo, utilice los recuadros de selección de cada fila para seleccionar una fila o para deseleccionar una fila, de modo que no se incluya en la llamada de API.
   Nota: Los parámetros con el nombre 'password' están enmascarados.
4. Utilice la lista desplegable para seleccionar el nivel de registro, que se representa lo siguiente: 0 - devuelve ID=identificador y ERR=código_error, como se ha definido en Códigos de devolución: 1 - muestra información adicional en la pantalla, 2 - coloca información en los registros de depuración de Guardium, 3 - realiza las dos acciones 1 y 2.
5. Utilice la lista desplegable para seleccionar un parámetro para cifrado.
   Nota: El cifrado de parámetros se habilita estableciendo el secreto compartido y solo es relevante para invocar la función de API a través de la generación de scripts.
6. Seleccione Invocar ahora o Generar script.
   a. Si selecciona Invocar ahora, la llamada de API se ejecuta inmediatamente y muestra una pantalla de salida de llamada de API con el estado de la llamada de API.
   b. Si selecciona Generar script
      i. Abra el script generado con su editor favorito o guárdelo en disco para editarlo y ejecutarlo más adelante.

         Script de ejemplo

         # A template script for invoking Sqlguard API function delete_datasource_by_name seven times:

         # Usage: ssh cli@a1.corp.com<delete_datasource_by_name_api_call.txt

         # replace any < > with the required value

         #

         set guiuser <username> password <password>

         grdapi delete_datasource_by_name name=192.168.2.91

         grdapi delete_datasource_by_name name=egret-oracle

         grdapi delete_datasource_by_name name=egret-oracle3

      ii. Modifique el script; sustituyendo cualquiera de los valores de parámetros vacíos (marcados con '< >')
         Nota: Es posible que los parámetros vacíos se conserven en el script, ya que la llamada de API los omite

         Script modificado de ejemplo

         # A template script for invoking Sqlguard API function delete_datasource_by_name seven times:

         # Usage: ssh cli@a1.corp.com<delete_datasource_by_name_api_call.txt

         # replace any < > with the required value

         #

         set guiuser <username> password <password>

         grdapi delete_datasource_by_name name=egret-oracle3

      iii. Ejecute la llamada a función de CLI

         Llamada de ejemplo

         $ ssh

         cli@a1.corp.com<c:/download/delete_datasource_by_name_api_call.txt

Correlacionar GuardAPI con los resultados de informes

Guardium incluye una batería de informes predefinidos y muchos de ellos ya se han correlacionado con las funciones de GuardAPI para facilitar la configuración. Además, Guardium permite a los usuarios definir informes adicionales, incluso sus propios informes personalizados, y correlacionarlos con funciones de GuardAPI por informe.

1. Vaya a cualquier informe predefinido en el separador Supervisor diario, en el separador Supervisor de Guardium o en el separador Supervisor Tap.
2. Pulse el botón Invocar...
3. Elija la selección Añadir correlación de API.
4. En la nueva ventana, Añadir correlación de API, se muestra el nombre del informe, por ejemplo, Inicios de sesión de Guardium, un mecanismo de búsqueda/filtro para buscar el mandato GuardAPI adecuado y las opciones de selección para las funciones de API disponibles en el informe predefinido. Seleccione la función de API y, a continuación, pulse Correlacionar atributos de informe.
5. En la nueva ventana, Correlacionar parámetros de informe de API, correlacione el nombre del parámetro con el campo Informe. En algunas ocasiones, es posible que algunos datos no se proporcionen con un informe de Guardium. En estos casos, se puede crear una constante, añadirla al informe y utilizarla en las correlaciones de parámetros de API.
   Nota: Si guarda, se reemplaza la correlación actual.
   Nota: Si se exporta el informe de Guardium con una constante añadida, la constante no se exportará.

Para simplificar la correlación entre los parámetros de GuardAPI y los atributos de Guardium, Guardium ha creado el informe predefinido Entidades y atributos que lista todos los atributos de Guardium que proporciona a los usuarios una interfaz de la GUI para obtener fácilmente más detalles de dicho informe y crear los enlaces rápidamente.

Los atributos de Guardium o las constantes definidas por el usuario se pueden correlacionar con los parámetros GuardAPI de los atributos o constantes existentes.

Nota: Cuando se correlacionan los parámetros GuardAPI con atributos de informe, si un informe tiene más de un atributo correlacionado con el mismo parámetro GuardAPI, el valor seleccionado para la llamada de API es el primero de estos atributos, según el orden de visualización del informe.

Atributos existentes

1. Vaya al informe Entidades y atributos de consulta para añadir las correlaciones de parámetros de API. (Supervisor de Guardium Monitor -> Entidades y atributos de consulta)
2. El informe Entidades y atributos de consulta es un informe largo, ya que lista todos los atributos de Guardium. Acote los registros que le interesan utilizando el botón Personalizar.
3. Para crear la correlación, pulse dos veces la fila de atributo que desee asignar a un nombre de parámetro
4. Pulse la opción Invocar...
5. Seleccione la función de API create_api_parameter_mapping
6. Rellene los parámetros functionName y parameterName en el formulario de llamada de API
7. Pulse Invocar ahora para crear la correlación de parámetros de API a informe

Consulte el tema sobre cómo utilizar las llamadas de API desde informes personalizados, para ver un escenario completo que correlaciona los parámetros de GuardAPI mediante la GUI.

Constantes

En algunas ocasiones, es posible que algunos datos no se proporcionen en un informe de Guardium. En estos casos, se puede crear una constante, añadirla al informe y utilizarla en las correlaciones de parámetros de API.

1. Vaya al informe Entidades y atributos de consulta para añadir las correlaciones de parámetros de API. (Supervisor de Guardium Monitor -> Entidades y atributos de consulta)
2. El informe Entidades y atributos de consulta es un informe largo, ya que lista todos los atributos de Guardium. Acote los registros que le interesan utilizando el botón Personalizar.
3. Para crear un atributo de constante, pulse dos veces cualquier fila de entidad para la que desee crear un atributo de constante
4. Pulse la opción Invocar...
5. Seleccione la función de API create_constant_attribute
6. Rellene el valor de constante que se va a utilizar y el valor de un attributeLabel al que desee asignar un nombre.
7. Pulse Invocar ahora para crear la constante.
8. Para crear la correlación, pulse dos veces la fila de atributos que ha creado
9. Pulse la opción Invocar...
10. Seleccione la función de API create_api_parameter_mapping
11. Rellene los parámetros functionName y parameterName en el formulario de llamada de API
12. Pulse Invocar ahora para crear la correlación de parámetros de API a informe
13. El atributo recién creado se debe añadir al informe. Modifique la consulta mediante el Creador de consultas y añada el campo.

Consulte el tema sobre cómo utilizar las constantes en llamadas de API, para ver un escenario completo que correlaciona un atributo de constante mediante la GUI.

Nota: Si se exporta el informe de Guardium con una constante añadida, la constante no se exportará.
Nota: Cuando se utiliza la correlación de API, las columnas de tabla de un informe aparecen en el campo de informe, siempre que la columna de tabla sea un atributo de una entidad. Algunas de las columnas, como por ejemplo la columna de recuento, no se visualizarán en el campo de informe porque no se puede correlacionar.

Seguridad de objetos para determinados mandatos de GuardAPI

La validación de roles implementa controles en mandatos de GuardAPI seleccionados para tener en cuenta los roles de los componentes específicos (y no sólo la aplicación) y no permitir acciones si los roles no coinciden.

Esto significa que un usuario que tiene los roles adecuados de Creador de políticas puede ejecutar el mandato delete_rule en cualquier política, independientemente de los roles de esta política específica.

Existe una validación de roles para los siguientes mandatos de reglas de política de GuardAPI: change_rule_order; copy_rule; copy_rules, delete_rule; update_rule.

Existe una validación de roles para los siguientes mandatos de descripción de grupo de GuardAPI: create_member_to_group_by_desc; create_member_to_group_by_id; delete_group_by_desc; delete_group_by_id; delete_member_from_group_by_desc; delete_member_from_group_by_id; update_group_by_id; update_group_by_desc.

Existe una validación de roles para los siguientes mandatos de origen de datos de GuardAPI: delete_datasource_by_id; delete_datasource_by_name; update_datasource_by_id; update_datasource_by_name.

Existe una validación de roles para los siguientes mandatos de proceso de auditoría de GuardAPI: stop_audit_process.

API para ejecutar un proceso de auditoría desde informes de tablas y gráficos

Se puede invocar GuardAPI automáticamente desde cualquier portlet de informe. Cuando se invoca GuardAPI, se crea un informe de proceso de auditoría nuevo.

Si existe dicho proceso para el usuario, se actualizan los parámetros y se utiliza el mismo proceso.

El comportamiento de GuardAPI es el siguiente:

1 - Si es un proceso nuevo, crea un receptor por correo electrónico de la lista (si hay alguno) con un tipo de contenido <p>, como se indica en el parámetro emailContentType. También crea un receptor de usuario para el usuario que ha iniciado sesión (invocando la API) si el parámetro includeUserReceiver es true.

2 - Si existe un proceso, se eliminan todos los destinatarios de correo electrónico y se sustituyen por los correos electrónicos de la nueva lista (si hay alguno) con el tipo de contenido que se ha definido en el parámetro emailContentType. Si la lista está vacía, elimina todos los destinatarios de la dirección de correo electrónico. Si ya existe un destinatario para el usuario, NO se eliminará, aunque el valor de includeUserreceiver sea false. Sin embargo, si el parámetro es true, dicho destinatario no existe.

Una vez generado el proceso de auditoría, se ejecuta automáticamente (similar a Ejecutar una vez ahora) y los usuarios deben esperar la recepción de un elemento en su lista de tareas pendientes para ese proceso de auditoría.

create_ad_hoc_audit_and_run_once

Parámetros:

1 - reportId: El ID del informe que se va a utilizar para la única tarea del proceso de auditoría

2 - isForReportRunOnce: Valor booleano que indica si se debe ejecutar el proceso una vez después de crearlo.

3 - changeParIfExist: Valor booleano que indica si se deben actualizar los parámetros de tareas si existe el proceso

4 - taskParameter: Todos los parámetros y el valor de cada uno concatenados con los caracteres ^^ deben escribirse de este modo: PAR1=Val1^^PAR2=Val2^^ etc. No es válido dejar un parámetro vacío, por ejemplo, si PAR2 debe estar vacío será similar al siguiente: PAR1=VAL1^^PAR2=^^PAR3=VAL3^^...

5 - processNamePar: El nombre del proceso, si está vacío se crea un proceso con el nombre.

6 - sendToEmails: Una lista separada por comas de direcciones de correo electrónico

7 - emailContentType: 0-PDF o 1-CSV (SOLO se aplica a destinatarios de correo electrónico)

8 - includeUserReceiver: Valor booleano que indica si se ha de crear un destinatario para el usuario que ha iniciado sesión.

Se puede invocar GuardAPI automáticamente desde cualquier portlet de informe. Cuando se invoca GuardAPI, se crea un informe de proceso de auditoría nuevo.

API de planificación

parámetros de modify_schedule jobName jobGroup cronString startTime opcional

list schedule

parámetros de delete_schedule jobName jobGroup deleteJob opcional

parámetros schedule_job jobType objectName opcional cronString startTime opcional

Nota: Algunos tipos de trabajo para la función schedule_job de grdapi no requieren un nombre de objeto. No se realiza ninguna validación en el parámetro de nombre de objeto y los usuarios ven una indicación de 'Aceptar' estándar cuando la función se ejecuta con cualquier entrada especificada como parámetro objectName para los siguientes tipos de trabajos: csvExportJob, dataArchiveJob, dataExportJob, dataImportJob, resultsArchiveJob, AppUserTranslation, IpHostToAlias

grdapi schedule_job --get_param_values=jobType - El valor del parámetro 'jobType' de la función 'schedule_job' debe ser uno de los siguientes: CustomTableDataUpload; AutoDetectProbeJob; AppUserTranslation; InstallPolicy: AuditJob; ResultArchive; AutoDetectScanJob; CustomTableDataPurge; CSVExport; DataExport; DataArchive; DataImport; PopulateGrpFromQry; SystemBackup; PopulateAlias; IpHostToAlias; UnitUtilization

grdapi set_purge_batch_size

Establece el tamaño del proceso por lotes que se utiliza durante la depuración, mejora al rendimiento de la depuración y tiene un valor predeterminado de 200.000. Se debe tener en cuenta la compensación de rendimiento y uso del espacio de disco, ya que cuando el valor del tamaño de proceso por lotes es más alto, se aumenta la velocidad de la depuración pero se consume más espacio de disco, y cuando el valor del tamaño de proceso por lotes es bajo se disminuye la velocidad de la depuración pero no se consume tanto espacio de disco.

parámetros de función: batchSize - necesario api_target_host Ejemplo: vx29> grdapi set_purge_batch_size batchSize=200000 ID=0 ok

grdapi get_purge_batch_size

Obtiene el valor actual del tamaño de proceso por lotes de depuración

parámetros de función: api_target_host Ejemplo: vx29> grdapi get_purge_batch_size ID=0 Purge Batch Size = 200000 ok

grdapi patch_install

parámetros de función: patch_date patch_number - necesario

grdapi populate_from_dependencies

parámetros de función: descOfEndingGroup - necesario descOfStartingGroup - necesario flattenNamespace getFunctions getJavaClasses getPackages getProcedures getSynonyms getTables getTriggers getViews isAppend - necesario isEndingGroupQualified owner - necesario reverseIt selectedDataSourceName - necesario api_target_host

create_computed_attribute

Utilizar en informes.

Tabla 1. create_computed_attribute

Parámetro	Descripción
attributeLabel	Necesario.
entityLabel	Necesario. Usuario de base de datos
expression	Necesario. IP de servidor Necesario. El usuario debe especificar tableName.field en la expresión.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

grdapi create_computed_attribute attributeLabel="CustomUserName" entityLabel="App User Name"
expression="SUBSTRING_INDEX(GDM_CONSTRUCT_INSTANCE.APP_USER_NAME,'.',1)"

delete_computed_attribute

Utilizar en informes.

Tabla 2. delete_computed_attribute

Parámetro	Descripción
attributeLabel	Necesario.
entityLabel	Necesario.
expression	Necesario.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

update_computed_attribute

Utilizar en informes.

Tabla 3. update_computed_attribute

Parámetro	Descripción
attributeLabel	Necesario.
entityLabel	Necesario.
expression	Necesario.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

create_constant_attribute

Utilizar en informes.

Tabla 4. create_constant_attribute

Parámetro	Descripción
attributeLabel	Necesario.
entityLabel	Necesario.
constant	Necesario.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

delete_constant_attribute

Utilizar en informes.

Tabla 5. delete_constant_attribute

Parámetro	Descripción
attributeLabel	Necesario.
entityLabel	Necesario.
constant	Necesario.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

update_constant_attribute

Utilizar en informes.

Tabla 6. update_constant_attribute

Parámetro	Descripción
attributeLabel	Necesario.
entityLabel	Necesario.
constant	Necesario.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

create_ad_hoc_audit_and_run_once

Utilizar en informes.

Tabla 7. create_ad_hoc_audit_and_run_once

Parámetro	Descripción
chnageParlfExist	Booleano. Necesario.
emailContentType	Entero
includeUserReceiver	Booleano
isForReportRunOnce	Booleano. Necesario.
processNamePar	Serie
reportID	Entero. Necesario
sendToEmails	Serie
taskParameter	Serie
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

API REST

La opción de salida JSON (JavaScript Object Notation) da soporte a las funciones de GuardAPI. Forma parte de las API REST. REST son las siglas de Representational State Transfer. Se basa en un protocolo de comunicaciones de cliente/servidor sin estado, que se puede colocar en memoria caché y, prácticamente en todos los casos, se utiliza el protocolo HTTP. REST es un estilo de arquitectura de diseño aplicaciones en red. La idea es que, en lugar de utilizar mecanismos complejos como, por ejemplo, CORBA, RPC o SOAP para la conexión entre máquinas, se utiliza HTTP simple para realizar llamadas entre máquinas. Las aplicaciones RESTful utilizan solicitudes HTTP para publicar datos (crear y actualizar), leer datos (por ejemplo, realizar consultas) y suprimir datos. Por lo tanto, REST utiliza HTTP para las cuatro operaciones Crear/Leer/Actualizar/Suprimir. REST es una alternativa ligera a mecanismos como RPC (Remote Procedure Calls) y servicios web (SOAP, WSDL).

Implementación de REST en Guardium

1. Registre la aplicación (sólo una vez) y obtenga el secreto de cliente.
2. Guarde el secreto del cliente en un lugar seguro.
3. Solicite la señal de acceso para autorización.
4. Guarde la señal de acceso, para el mandato grdAPI se autentique correctamente.
5. Utilice las señales de acceso para mandatos de GuardAPI.

Casos de uso de ejemplo

- Deseo obtener dinámicamente una pequeña cantidad de datos de auditoría para una dirección IP determinada sin tener que iniciar sesión en la GUI de Guardium.
- Deseo rellenar un grupo existente, de modo que pueda actualizar mi política para impedir el acceso no autorizado a la información confidencial.
- Deseo obtener una lista de todos los usuarios de un determinado grupo de acceso autorizado.
- Deseo que mi equipo de desarrollo de aplicaciones ayude a identificar qué tablas confidenciales se deben supervisar.
- Deseo escribir un script para acceder a las grdAPI sin utilizar el lenguaje de script "expect", que requiere codificar texto de respuesta desde el sistema de destino.

HTTP tiene un vocabulario de operaciones (métodos de solicitud)

- GET (pasar parámetros en el URL)
- POST (pasar parámetros en un objeto JSON)
- PUT (pasar parámetros para cambiar como objeto JSON)
- DELETE (pasar parámetros como objeto JSON)

Usuario especial para solicitudes de API REST

Para las solicitudes internas de API REST, hay un ROLE y USER especiales predefinidos en el sistema.

Este usuario no se puede eliminar ni modificar mediante la IU accessmgr y no se puede utilizar para iniciar la sesión en la IU.

La contraseña de este usuario no caduca nunca, pero se revoca si se revoca el ID de cliente.

En el registro del cliente OAuth, una nueva función acepta este ID de usuario y de cliente. Genera una contraseña fuerte aleatoria para el usuario y la almacena en la tabla TURBINE_USER.

Devuelve un secreto de cliente y la contraseña generada.

El cliente interno (S-TAP, quizás otros) debe proteger el secreto y la contraseña del cliente.

Los permisos para las distintas funciones se pueden asignar al rol mediante IU accessmgr.

Comparación de RestAPI con. GuardAPI

GET = Listar

POST = Crear

PUT = Actualizar

DELETE = Suprimir

GuardAPI

```
list_datasourcename_by_name (parameters - ?name="MSSQL_1")
```

```
-X GET https://10.10.9.239:8443/restAPI/datasource/?name="MSSQL_1"
```

create_datasource

```
-X POST https://10.10.9.239:8443/restAPI/datasource
```

```
update_datasource_by_name - JSON Object '{password:guardium}'
```

```
-X PUT -d '{password:guardium, name:"MSSQL_1}'
```

```
delete_datasource_by_id - JSON Object '{"id":20020}'
```

```
-X DELETE -d '{"id":20020}'
```

Para obtener más información, consulte el tema Utilización de la API REST de IBM Security Guardium en DeveloperWorks.

http://www.ibm.com/developerworks/data/library/techarticle/dm-1404guardrestapi/index.html

Consultar y reiniciar una hebra UnitPinger interna

Utilice este mandato GuardAPI para consultar y reiniciar una hebra UnitPinger interna.
NOTA: Este mandato GuardAPI se ha de invocar con el parámetro api_target_host=127.0.0.1.
Ejemplo
grdapi get_unit_pinger api_target_host=127.0.0.1

register_oauth_client

Utilice este mandato GuardAPI para incluir las funciones GuardAPI soportadas en una API RESTful que utilice JSON (JavaScript Object Notation) como entrada y salida.

Utilice el mandato GrdAPI, grdapi register_oauth_client, para registrar el cliente y obtener la señal de acceso necesaria para invocar los servicios REST.

REST son las siglas de Representational State Transfer. Se basa en un protocolo de comunicaciones de cliente/servidor sin estado, que se puede colocar en memoria caché y, prácticamente en todos los casos, se utiliza el protocolo HTTP.

REST es un estilo de arquitectura de diseño aplicaciones en red. La idea es que, en lugar de utilizar mecanismos complejos como, por ejemplo, CORBA, RPC o SOAP para la conexión entre máquinas, se utiliza HTTP simple para realizar llamadas entre máquinas.

Las aplicaciones RESTful utilizan solicitudes HTTP para publicar datos (crear y actualizar), leer datos (por ejemplo, realizar consultas) y suprimir datos. Por lo tanto, REST utiliza HTTP para las cuatro operaciones Crear/Leer/Actualizar/Suprimir. REST es una alternativa ligera a mecanismos como RPC (Remote Procedure Calls) y servicios web (SOAP, WSDL).

parámetros de función:

client_id - Serie - necesario

grant_types - Serie - necesario. El único tipo grant al que se da soporte es password.

redirect_uris - Serie - necesario

scope - Serie - necesario.

fetchSize - Serie- opcional (el valor predeterminado es 20 para mantener la compatibilidad con versiones anteriores, el valor máximo es 30000.

sortColumn - opcional - Si se especifica, debe ser el título de columna de uno de los campos de informe.

sortType - opcional - asc o desc

Sintaxis

grdapi register_oauth_client <client_id> <grant_types> <redirect_uris> <scope>

getOAuthTokenExpirationTime

Utilice este mandato GuardAPI para obtener la hora de caducidad de la señal de la API REST

parámetros de función:

api_target_host - Serie

setOAuthTokenExpirationTime

Utilice este mandato GuardAPI para establecer la hora de caducidad de la señal de la API REST.

parámetros de función:

expirationTime - Entero - necesario

api_target_host - Serie

Sintaxis

grdapi setOAuthTokenExpirationTime ExpirationTime=10000

Tema principal: Referencia de GuardAPI

Funciones del panel de control de investigación de GuardAPI

Utilice estos mandatos de GuardAPI para habilitar, inhabilitar o configurar parámetros y características del panel de control de investigación.

disable_quick_search

Tenga en cuenta que el panel de control de investigación incluye la tabla de resultados de búsqueda rápida, junto con el gráfico de actividad y otros gráficos predefinidos.

Inhabilitar las funciones del panel de control de investigación.

```
grdapi disable_quick_search
```

Parámetro	Valor	Descripción
all	`true` o `false`	En un entorno con un Gestor central, utilice este parámetro para inhabilitar la búsqueda en todas las unidades gestionadas. Por ejemplo, `all=true`. Este parámetro es opcional.
api_target_host	hostname o dirección IP	Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM. Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Este parámetro es opcional.

enable_quick_search

Habilitar las funciones del panel de control de investigación.

```
grdapi enable_quick_search schedule_interval=[value] schedule_units=[value]
```

Por ejemplo, el mandato siguiente habilita el panel de control de investigación con un intervalo de extracción de datos de 2 minutos: `grdapi enable_quick_search schedule_interval=2 schedule_units=MINUTE`.

Parámetro	Valor	Descripción
all	`true` o `false`	En un entorno con un Gestor central, utilice este parámetro para habilitar la búsqueda en todas las unidades gestionadas. Por ejemplo, `all=true`. Este parámetro es opcional.
api_target_host	hostname o dirección IP	Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM. Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Este parámetro es opcional.
extraction_start	date	Defina la fecha en que se iniciará la extracción de los datos de auditoría para la búsqueda. Si se omite este parámetro, la extracción se inicia inmediatamente. Este parámetro es opcional.
includeViolations	`true` o `false`	Determinar si se deben incluir infracciones en los índices de búsqueda. Omitir infracciones ayuda a reducir el tamaño de los índices de búsqueda. Este parámetro es opcional.

schedule_interval	entero	Se utiliza con el parámetro schedule_units para definir el intervalo para la extracción de datos de auditoría. Por ejemplo, `schedule_interval=2 schedule_units=MINUTE`. Este parámetro es necesario.
schedule_start	date	Fecha en la que se empieza a seguir el intervalo de extracción definido por los parámetros schedule_interval y schedule_units. Este parámetro es opcional.
schedule_units	`HOUR` o `MINUTE`	Se utiliza con el parámetro schedule_interval para definir el intervalo para la extracción de datos de auditoría. Por ejemplo, `schedule_interval=2 schedule_units=MINUTE`. Este parámetro es necesario.

set_enterprise_search_options

Definir la modalidad de búsqueda para el panel de control de investigación.

```
grdapi set_enterprise_search_options distributed_search=[value]
```

Por ejemplo, el mandato siguiente configura el panel de control de investigación en modalidad all_machines para permitir la búsqueda de datos en todo el entorno de Guardium, desde cualquier máquina de Guardium: `grdapi set_enterprise_search_options distributed_search=all_machines`.

Parámetro	Valor	Descripción
api_target_host	hostname o dirección IP	Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM. Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Este parámetro es opcional.
distributed_search	cm_only, local_only o all_machines	cm_only Las búsquedas enviadas desde un gestor central devuelven los resultados de todo el entorno de Guardium, pero las búsquedas enviadas desde unidades gestionadas solo devuelven los resultados locales de las unidades gestionadas local_only Las búsquedas enviadas desde máquinas individuales solo devuelven los resultados de dicha máquina. No hay ninguna posibilidad de buscar datos en el entorno de Guardium. all_machines Las búsquedas se pueden enviar desde cualquier máquina y se devuelven los resultados de todo el entorno Guardium. Este parámetro es necesario y el valor predeterminado es cm_only.

Tema principal: Referencia de GuardAPI

Funciones de auditoría nativas de GuardAPI

Utilice estos mandatos GuardAPI para habilitar, inhabilitar, la auditoría de base de datos (auditoría nativa) en la nube, para añadir y eliminar objetos de la auditoría nativa y para obtener objetos de configuración, recopiladores y objetos.

add_ip_to_sg

Añade la IP de Guardium especificada al grupo de seguridad de la nube.

```
add_objects_native_audit parameter=value
```

Parámetro	Valor	Descripción
datasource_name	Serie.	Necesario. El nombre del origen de datos de nube definido en Guardium
api_target_host	Serie.	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM)

add_objects_native_audit

Añade objetos a la Auditoría de objetos (seguimiento de auditoría) en el origen de datos especificado.

```
add_objects_native_audit parameter=value
```

Parámetro	Valor	Descripción
datasource_name	Serie.	Necesario. El nombre del origen de datos de nube definido en Guardium
objects	Serie.	Lista de objetos separados por comas. Objetos de visualización con get_native_audit_objects o en la interfaz gráfica de usuario.
api_target_host	Serie.	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM)

disable_native_audit

Inhabilita la auditoría de base de datos (auditoría nativa) en el origen de datos de nube especificado.

```
disable_native_audit parameter=value
```

Parámetro	Valor	Descripción
datasource_name	serie	Necesario. El nombre del origen de datos de nube definido en Guardium
api_target_host	serie	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM)

enable_native_audit

Habilita la auditoría de base de datos (auditoría nativa) en el origen de datos especificado.

```
enable_native_audit parameter=value
```

Parámetro	Valor	Descripción
datasource_name	serie	Necesario. El nombre del origen de datos de nube definido en Guardium
api_target_host	serie	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM)

get_native_audit_collectors

Devuelve el nombre del recopilador, en su entorno, que está recibiendo datos desde el nombre de servicio, puerto y host especificados.

```
get_native_audit_collectors parameter=value
```

Parámetro	Valor	Descripción
host	serie	Necesario. Nombre de host AWS.
port	entero	Necesario.
service_name	serie	Necesario.
api_target_host	serie	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas

		• all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM)

get_native_audit_configurations

Devuelve todos los detalles en el nombre de servicio, puerto y host especificados: ID de entorno de nube, entorno de nube, proveedor, ID de origen de datos, nombre de instancia, motor de base de datos, nombre de servicio, host, puerto, grupo de seguridad de Guardium, límite de objetos, objetos, recopilador.

`get_native_audit_configurations parameter=value`

Parámetro	Valor	Descripción
host	serie	Necesario. Nombre de host AWS.
port	entero	Necesario.
service_name	serie	Necesario.
api_target_host	serie	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM)

get_native_audit_objects

Devuelve todos los objetos encontrados por el proceso de clasificación en el nombre de servicio, puerto y host especificados.

`get_native_audit_objects parameter=value`

Parámetro	Valor	Descripción
host	serie	Necesario. Nombre de host AWS.
port	entero	Necesario.
service_name	serie	Necesario.
api_target_host	serie	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM)

remove_objects_native_audit

Inhabilita la auditoría de objetos (seguimiento de auditoría) en los objetos especificados en el origen de datos especificado.

`remove_objects_native_audit parameter=value`

Parámetro	Valor	Descripción
datasource_name	serie	Necesario. El nombre del origen de datos de nube definido en Guardium
objects	serie	Lista de objetos separados por comas. Objetos de visualización con get_native_audit_objects o en la interfaz gráfica de usuario.
api_target_host	serie	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM)

Tema principal: Referencia de GuardAPI

Funciones de detección de valores atípicos de GuardAPI

Utilice los mandatos GuardAPI siguientes para habilitar, inhabilitar y configurar la función de detección de valores atípicos.

grdapi enable_outliers_detection_agg

grdapi enable_outliers_detection_agg

grdapi disable_outliers_detection_agg

Se ejecuta en un gestor central para habilitar o inhabilitar el envío de datos de exportación desde todos los recopiladores del entorno de CM que envían sus datos al agregador especificado, excepto un recopilador que está ejecutando localmente la detección de valores atípicos. Los datos se recopilan cada hora y se envían al agregador para el proceso de detección de valores atípicos. Se utiliza un mecanismo de informe distribuido para extraer y enviar datos a un agregador.

Tabla 1. grdapi enable_outliers_detection_agg

Parámetro	Descripción
schedule_interval	Obligatorio. Se debe establecer en 1
schedule_units	Obligatorio. Se debe establecer en hour
aggregator_host_name	El agregador específico habilitado o inhabilitado para la detección de valores atípicos.
DAM_FAM	Opcional. Especifica el tipo de valores atípicos. El valor predeterminado es DAM.

grdapi enable_outliers_detection

grdapi enable_outliers_detection

grdapi disable_outliers_detection

Se ejecuta en un recopilador para habilitar o inhabilitar la detección de valores atípicos localmente en el recopilador.

Tabla 2. grdapi enable_outliers_detection

Parámetro	Descripción
schedule_interval	Obligatorio. Se debe establecer en 1
schedule_units	Obligatorio. Se debe establecer en hour
DAM_FAM	Opcional. Especifica el tipo de valores atípicos. El valor predeterminado es DAM.

grdapi set_outliers_detection_parameter privUsersGroupIds

Añadir grupos de usuarios adicionales al algoritmo de detección de valores atípicos. Utilice este mandato para buscar un ID de grupo: grdapi list_group_by_desc desc=[nombre grupo]

Tabla 3. grdapi set_outliers_detection_parameter

Parámetro	Descripción
privUsersGroupIds	Uno o varios ID de grupo de usuarios admin.
sensitiveObjectGroupIds	Uno o varios ID de grupo de usuarios confidenciales.

Tema principal: Referencia de GuardAPI

Funciones de control de procesos de GuardAPI

Utilice estos mandatos GuardAPI para ejecutar, copiar, cargar, listar y suprimir las funciones de control de procesos.

Ejecutar (enviar) un proceso de clasificación

Ejecuta un proceso de clasificación. Es equivalente a Ejecutar una vez ahora en el Creador de procesos de clasificación. Envía el trabajo que coloca el proceso en la cola de trabajos de Guardium, desde la que el dispositivo ejecuta un solo trabajo cada vez. Los administradores pueden ver el estado del trabajo seleccionado Supervisor de Guardium > Cola de trabajos de Guardium.

Nota: Cree un proceso de clasificación antes de invocar esta API.

Tabla 1. Ejecutar (enviar) un proceso de clasificación

Parámetro	Descripción
processName	Nombre del proceso de clasificación

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi execute_cls_process processName="classPolicy1"
```

Ejecutar (enviar) un asesoramiento de clasificación

Ejecuta el asesoramiento especificado. Es equivalente a Ejecutar una vez ahora en el Buscador de asesoramientos de seguridad. Envía el trabajo. Este trabajo coloca el proceso en la cola de trabajos de Guardium, desde la que el dispositivo ejecuta un solo trabajo cada vez. Los administradores pueden ver el estado del trabajo seleccionado Supervisor de Guardium > Cola de trabajos de Guardium.

Nota: Cree un asesoramiento de seguridad antes de invocar esta API.

Tabla 2. Ejecutar (enviar) un asesoramiento de clasificación

Parámetro	Descripción
assessmentDesc	Nombre del asesoramiento
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi execute_assessment assessmentDesc="assessment1"
```

Ejecutar un proceso de auditoría

Ejecuta un proceso de auditoría. Ejecuta el proceso de auditoría especificado. Es equivalente a Ejecutar una vez ahora en el Creador de procesos de auditoría.

Nota: Cree un proceso de auditoría antes de invocar esta API.
Nota: Si el informe de auditoría devuelve una gran cantidad de datos, el usuario debe ejecutar el proceso de auditoría desde la GUI, debido al límite de tamaño de almacenamiento dinámico de mandatos de CLI.

Tabla 3. Ejecutar un proceso de auditoría

Parámetro	Descripción
auditProcess	Nombre del proceso de auditoría
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi execute_auditProcess  auditProcess="Appliance Monitoring"
```

Detener un proceso de auditoría

La API stop_audit_process no se puede utilizar mediante la línea de mandatos de GuardAPI. Esta función solo se puede utilizar como una invocación mediante detallar más. Consulte el subtema, Detener un proceso de auditoría, en el tema de ayuda Conformidad de la automatización de la carga de trabajo.

Tabla 4. Detener un proceso de auditoría

Parámetro	Descripción
process	Nombre del proceso de auditoría
run	El ID de ejecución del proceso de auditoría
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
stop_audit_process
```

Cumplimentar grupo desde consulta

Cumplimenta el grupo elegido ejecutando una consulta configurada. Es equivalente a Ejecutar una vez ahora en la pantalla Cumplimentar grupo desde configuración de consulta. Si el grupo no está configurado para su importación, se muestra un mensaje de error.

Nota: Este mandato grdapi sólo se puede utilizar para los grupos que ya se han configurado en la pantalla Cumplimentar grupo desde configuración de consulta (la consulta debe estar seleccionada y los parámetros establecidos).

Tabla 5. Cumplimentar grupo desde consulta

Parámetro	Descripción
groupDesc	Nombre de grupo
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi execute_populateGroupFromQuery  groupDesc="A test"
```

Ejecutar una conversión de usuarios de aplicación

Importa las definiciones de usuario para todas las aplicaciones configuradas en la pantalla Configuración de la conversión de usuarios de aplicación. Es equivalente a Ejecutar una vez ahora en la pantalla Configuración de la conversión de usuarios de aplicación.

Nota: Para ejecutar esta función de grdapi, debe definir al menos una detección de usuarios de aplicación en la pantalla Configuración de la conversión de usuarios de aplicación. De lo contrario, se muestra un mensaje.

Tabla 6. Ejecutar una conversión de usuarios de aplicación

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi execute_appUserTranslation
```

Ejecutar un proceso flat log

Fusiona la información de flat log con la base de datos interna. Es equivalente a Ejecutar una vez ahora en la pantalla Proceso Flat Log.

Nota: Esta función grdapi solo se puede ejecutar si el proceso Flat Log se ha configurado como proceso en la pantalla Proceso Flat Log. De lo contrario, se muestra un mensaje de error.

Tabla 7. Ejecutar un proceso flat log

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi execute_flatLogProcess
```

Ejecutar proceso de generación de incidencias

Ejecuta una consulta definida para el proceso de generación de incidencias seleccionado, en el registro de infracciones de política. Genera incidencias basadas en dicha consulta. Es equivalente a Ejecutar una vez ahora en la pantalla Editar proceso de generación de incidencias.

Nota: Cree un Proceso de generación de incidencias antes de invocar esta API.

Dado que el proceso de generación de incidencias no tiene un nombre exclusivo, para diferenciar uno específico, se puede utilizar un processId o un queryName.

Hay dos métodos de invocar esta grdapi:

- execute_incidentGenProcess
- execute_incidentGenProcess_byDetails

Tabla 8. Ejecutar proceso de generación de incidencias

Parámetro	Descripción
processID	ID de proceso de la incidencia
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi execute_incidentGenProcess   processId=20003
```

Tabla 9. execute_incidentGenProcess_byDetails

Parámetro	Descripción
queryName	Nombre de la consulta
categoryName	Nombre de categoría
user	Usuario
threshold	Umbral
severity	Nivel de gravedad

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi  execute_incidentGenProcess_byDetails  queryName="Policy Violation Count" user=admin severity=info
```

Cargar datos personalizados - ejecuta (envía) un proceso de clasificación

Carga datos en la tabla personalizada especificada mediante tableName. Es equivalente a ejecutar Cargar en la pantalla Importar datos del creador de tablas personalizadas. Para ejecutar esta grdapi, en primer lugar, debe configurar la tabla personalizada especificada en Importar estructura de datos del creador de tablas personalizadas. En la IU, vaya a Herramientas/Creador de informes/Creador de tablas personalizadas, seleccione una tabla personalizada, pulse Subir datos y seleccione el origen de datos.

Nota: tableName especifica el nombre de una tabla personalizada existente.

Tabla 10. Cargar datos personalizados - ejecuta (envía) un proceso de clasificación

Parámetro	Descripción
tableName	Nombre de la tabla personalizada
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi upload_custom_data tableName="TEST_TABLE"
```

Importar usuarios LDAP

Importa las definiciones de usuario de Guardium de un servidor LDAP configurado en la pantalla Importar usuarios LDAP. Es equivalente a Ejecutar una vez ahora en la pantalla Importar usuarios LDAP. (inicie sesión como accessmgr/Importar LDAP)

Nota: LDAP debe estar configurado. De lo contrario, el sistema muestra un mensaje de error.

Tabla 11. Importar usuarios LDAP

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi execute_ldap_user_import
```

Instalar política

Instalar una política o varias políticas. Si se van a instalar varias políticas, las políticas deben delimitarse mediante un carácter de barra vertical '|' con las políticas en el orden en que desea que se instalen. Esto se debe realizar incluso si solo se ha modificado una política.

Instale varias políticas con el mandato grdapi policy_install. Instale por posición especificando las políticas en el orden que desea instalarlas.

Incluso en la IU, cuando se instala una política después de otra política instalada, se reinstalan todas. Lo cual es mismo que el mandato grdapi policy_install.

Tabla 12. Instalar política

Parámetro	Descripción
policy	Nombre de política
api_target_host	Solo en una configuración de gestión central, permite al usuario especificar un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplos

```
grdapi policy_install policy="Policy 1|Policy 2"
```

```
grdapi policy_install policy="policy 20|policy 30|policy 40"
```

Suprimir política

Utilice el mandato delete_policy para suprimir una política especificada mediante el parámetro policyDesc.

Tabla 13. Suprimir política

Parámetro	Descripción
policyDesc	Nombre de la política.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi delete_policy policyDesc="Hadoop Policy"
```

Listar políticas

Utilice el mandato list_policy para visualizar una lista de políticas disponibles o para visualizar detalles sobre una sola política.

Tabla 14. Listar políticas

Parámetro	Descripción
policyDesc	Nombre de la política. Si no se especifica, el mandato list_policy devuelve una lista de las políticas disponibles.
detail	Acepta los valores true o false. El valor predeterminado es true que devuelve los detalles de la política. Si se especifica el valor false, solo se devuelven los nombres de políticas.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplos

Mostrar detalles de una política específica:

```
grdapi list_policy policyDesc="Hadoop Policy"
```

Mostrar una lista detallada de las políticas disponibles:

```
grdapi list_policy
```

Mostrar una lista de nombres de políticas disponibles (sin detalles):

```
grdapi list_policy detail=false
```

Copiar regla de política

Copiar un regla <ruleDesc> de <fromPolicy> al final de la lista de la regla <toPolicy>.

Nota: Copia una regla <fromPolicy> al final de la lista de la regla <toPolicy>. Antes de ejecutar esta grdapi, se deben haber creado <fromPolicy> y <toPolicy>.

Tabla 15. Copiar regla de política

Parámetro	Descripción
ruleDesc	Descripción de regla
fromPolicy	Nombre de política
toPolicy	Nombre de política
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi copy_rule ruleDesc="Rule Description" fromPolicy="policy1"  toPolicy=" policy2  "
```

Clonar política

Utilice este mandato GuardApi para clonar una política.

Tabla 16. Clonar política

Parámetro	Descripción
policyDesc	Nombre de política
clonedpolicyDesc	Nombre de la política clonada
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi clone_policy policyDesc="Hadoop Policy" clonedPolicyDesc="Hadoop Policy cloned1"
```

Actualizar regla de política

Actualizar una regla <ruleDesc> de <fromPolicy> para un parámetro de regla.

Consulte la sección Políticas para obtener información adicional sobre los parámetros de reglas de políticas que se pueden modificar invocando la API update_rule.

Tabla 17. Actualizar regla de política

Parámetro	Descripción
ruleDesc	Descripción de regla
fromPolicy	Nombre de política
newDesc	Descripción de la regla nueva
clientIP	IP de cliente
clientNetMask	Máscara de red de cliente
serverIP	IP de servidor
serverNetMask	Máscara de red de servidor
objectName	Nombre de objeto
sourceProgram	Programa de origen
dbName	Nombre de base de datos
dbUser	Usuario de base de datos
command	Mandato

Parámetro	Descripción
appUserName	Nombre de usuario de aplicación
dateTime	Fecha y hora
logFlag	Distintivo de registro
exceptionType	Tipo de excepción
minCount	Recuento mínimo
continueToNext	Continuar con el siguiente
resetInterval	Intervalo de restablecimiento
serviceName	Nombre de servicio
osUser	Usuario de S/O
dbType	Tipo de base de datos
netProtocol	Protocolo de red
clientMac	MAC de cliente
fieldName	Nombre de campo
pattern	Patrón
appEventExists	Existe un suceso de aplicación
eventType	Tipo de suceso
appEventStrValue	Valor de serie de suceso de aplicación
appEventNumValue	Valor numérico de suceso de aplicación
appEventDate	Fecha de suceso de aplicación
eventUserName	Nombre de usuario de suceso
errorCode	Código de error
severity	Gravedad
category	Categoría
classification	Clasificación
dataPattern	Patrón de datos
sqlPattern	Patrón SQL
xmlPattern	Patrón XML
mvcSystem	Sistema MVS
clientIpNotFlag	IP de cliente sin distintivo
serverIpNotFlag	IP de servidor sin distintivo
objectNameNotFlag	Nombre de objeto sin distintivo
sourceProgramNotFlag	Programa de origen sin distintivo
dbNameNotFlag	Nombre de base de datos sin distintivo
dbUserNotFlag	Usuario de base de datos sin distintivo
commandNotFlag	Mandato sin distintivo
appUserNameNotFlag	Nombre de usuario de aplicación sin distintivo
exceptionTypeIdNotFlag	ID de tipo de excepción sin distintivo
serviceNameNotFlag	Nombre de servicio sin distintivo
osUserNotFlag	Usuario de S/O sin distintivo
clientMacNotFlag	MAC de cliente sin distintivo
fieldNameNotFlag	Nombre de campo sin distintivo
errorCodeNotFlag	Código de error sin distintivo
replacementChar	Carácter de sustitución
messageTemplate	Plantilla de mensaje
recordsAffectedThreshold	Umbral de registros afectados
matchedReturnedTreshold	Umbral de devoluciones coincidentes
clientIpGroup	Grupo de IP de cliente
serverIpGroup	Grupo de IP de servidor
objectGroup	Grupo de objetos
objectCommandGroup	Grupo de mandatos de objeto
objectFieldGroup	Grupo de campos de objeto
dbUserGroup	Grupo de usuarios de base de datos

Parámetro	Descripción
commandsGroup	Grupo de mandatos
dbNameGroup	Grupo de nombres de base de datos
sourceProgramGroup	Grupo de programas de origen
appUserGroup	Grupo de usuarios de aplicación
serviceNameGroup	Grupo de nombres de servicio
osUserGroup	Grupo de usuarios de S/O
netProtocolGroup	Grupo de protocolos de red
fieldNameGroup	Grupo de nombres de campo
errorGroup	Grupo de errores
appEventStrGroup	Grupo de series de sucesos de aplicación
clientProgramUserServerInstanceGroup	Grupo de instancias de servidor de usuarios del programa cliente
quarantineMinutes	Minutos de cuarentena
clientInfo	Utilizar para DB2 y DB2_COLLECTION_PROFILE
clientInGroup	Utilizar para DB2_COLLECTION_PROFILE
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi update_rule ruleDesc="Rule Description" fromPolicy="policy1"  serviceName="ANY"
```

Cambiar orden de regla de política

Cambiar la posición de clasificación de una regla en una política.

Tabla 18. Cambiar orden de regla de política

Parámetro	Descripción
fromPolicy	Nombre de política
order	Nueva posición de orden para la regla
ruleDesc	Descripción de regla
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi change_rule_order ruleDesc="Copy of policy1 exception1"  fromPolicy="policy1"  order=10
```

Listar reglas de política

Listar las reglas de una política.

Tabla 19. Listar reglas de política

Parámetro	Descripción
policy	Nombre de política

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi list_policy_rules  policy="policy1"
```

Suprimir regla de política

Eliminar una regla de una política.

Tabla 20. Suprimir regla de política

Parámetro	Descripción
fromPolicy	Nombre de política
toPolicy	Nombre de política
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi delete_rule ruleDesc="Copy (3) of policy1 exception1"  fromPolicy="policy1"
```

Desinstalar regla de política

Utilice el mandato uninstall_policy_rule para desinstalar las reglas de política especificadas con los parámetros policy y ruleName.

Tabla 21. Volver a instalar regla de política

Parámetro	Descripción
policy	Nombre de la política.
ruleName	Nombre de reglas de políticas. Especifique varias reglas de política utilizando el carácter de barra vertical, por ejemplo: `ruleName="rule1|rule2|rule3`.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplos

Desinstalar una sola regla de política:

```
grdapi uninstall_policy_rule policy="Hadoop Policy" ruleName="Low interest Objects: Allow"
```

Desinstalar varias reglas de política:

```
grdapi uninstall_policy_rule policy="Hadoop Policy" ruleName="Low interest Objects: Allow|Low Interest Commands: Allow"
```

Volver a instalar regla de política

Utilice el mandato reinstall_policy_rule para volver a instalar las reglas de política especificadas con los parámetros policy y ruleName.

Tabla 22. Volver a instalar regla de política

Parámetro	Descripción
policy	Nombre de la política.
ruleName	Nombre de reglas de políticas. Especifique varias reglas de política utilizando el carácter de barra vertical, por ejemplo: `ruleName="rule1|rule2|rule3`.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplos

Volver a instalar una sola regla de política:

```
grdapi reinstall_policy_rule policy="Hadoop Policy" ruleName="Low interest Objects: Allow"
```

Volver a instalar varias reglas de política:

```
grdapi reinstall_policy_rule policy="Hadoop Policy" ruleName="Low interest Objects: Allow|Low Interest Commands: Allow"
```

Suprimir resultados del proceso de auditoría

Utilice este mandato para suprimir cualquier resultado del proceso de auditoría.

Tabla 23. Suprimir resultados del proceso de auditoría

Parámetro	Descripción
ExecutionDateFrom	La fecha de inicio del proceso de auditoría
ExecutionDateTo	La fecha de finalización del proceso de auditoría
ProcessName	Necesario. El nombre del proceso de auditoría
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi delete_Audit_process_result ExecutionDateFrom=, ExecutionDateTo=, ProcessName=abab
```

Correlacionar parámetros de API con entidades y atributos de dominio

Correlacione los parámetros de API con atributos y entidades de dominio para que los parámetros se puedan llenar mediante valores de informe cuando se generan llamadas a API o de automatización de API.

Nota: La correlación de parámetros de GuardAPI con entidades y atributos en la generación de procesos de entrada de GuardAPI muestra los dominios, entidades y atributos del sistema y tiene una interfaz GUI para invocar esta función de API.

Tabla 24. Correlacionar parámetros de API con entidades y atributos de dominio

Parámetro	Descripción
functionName	Nombre de la función de API
parameterName	Nombre del parámetro en la función de API que se va a correlacionar
domain	Cualquiera de los dominios de informe de Guardium como, por ejemplo, Acceso, Alerta, Instancias descubiertas, Excepciones, Seguimiento de grupos, etc.
entityLabel	Cualquiera de las entidades del dominio de informes
attributeLabel	Cualquiera de los atributos de la entidad

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi create_api_parameter_mapping functionName="create_group" parameterName="desc" domain="Group Tracking" entityLabel="Group"
attributeLabel="Group Description"
```

Listar correlaciones de parámetros de API con entidades y atributos de dominio

Listar las correlaciones de parámetros de una función de API.

Nota: La correlación de parámetros de GuardAPI con entidades y atributos en la generación de procesos de entrada de GuardAPI muestra los dominios, entidades y atributos del sistema y tiene una interfaz GUI para invocar esta función de API.

Tabla 25. Listar correlaciones de parámetros de API con entidades y atributos de dominio

Parámetro	Descripción
functionName	Nombre de la función de API
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi list_param_mapping_for_function functionName="create_group"
```

Suprimir correlaciones de parámetros de API con entidades y atributos de dominio

Eliminar las correlaciones de parámetros de una función de API.

Nota: La correlación de parámetros de GuardAPI con entidades y atributos en la generación de procesos de entrada de GuardAPI muestra los dominios, entidades y atributos del sistema y tiene una interfaz GUI para invocar esta función de API.

Tabla 26. Suprimir correlaciones de parámetros de API con entidades y atributos de dominio

Parámetro	Descripción
functionName	Nombre de la función de API
parameterName	Nombre del parámetro en la función de API que se va a correlacionar
domain	Cualquiera de los dominios de informe de Guardium como, por ejemplo, Acceso, Alerta, Instancias descubiertas, Excepciones, Seguimiento de grupos, etc.
entityLabel	Cualquiera de las entidades del dominio de informes
attributeLabel	Cualquiera de los atributos de la entidad
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi delete_api_parameter_mapping functionName="create_group" parameterName="desc" domain="Group Tracking" entityLabel="Group"
attributeLabel="Group Description"
```

Cerrar todos los sucesos definidos en un proceso/tarea/ejecución específico

Cerrar todos los sucesos definidos en un proceso/tarea/ejecución específico para tareas de informe de tipo. Es especialmente necesario si, por ejemplo, hay una tarea con un suceso predeterminado que ha devuelto un gran número de registros, dicha tarea no se puede firmar a menos que todos los sucesos estén cerrados.

Tabla 27. Cerrar todos los sucesos definidos en un proceso/tarea/ejecución específico

Parámetro	Descripción
eventStatus	Necesario. Estado del suceso. Debe ser un estado válido para el suceso predeterminado definido para la tarea de auditoría y debe ser un estado final.
execDate	Necesario. Fecha y hora de la ejecución
processDesc	Necesario. Descripción del proceso de auditoría.
taskDesc	Necesario. Descripción de la tarea de auditoría.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi close_default_events eventStatus=Done execDate="2010-03-01 08:00:00" processDesc="Audit Process" taskDesc="Task
Description"
```

create_quarantine_allowed_until

Utilizar en políticas.

Tabla 28. create_quarantine_allowed_until

Parámetro	Descripción
allowedUntil	Necesario.
dbUser	Necesario. Usuario de base de datos
serverIP	Necesario. IP de servidor
serverName	Necesario. Nombre de servidor
Type	Necesario. El valor debe ser: normal, DB2z o IMS.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

create_quarantine_until

Utilizar en políticas.

Tabla 29. create_quarantine_until

Parámetro	Descripción
quarantineUntil	Necesario.
dbUser	Necesario. Usuario de base de datos
serverIP	Necesario. IP de servidor
serverName	Necesario. Nombre de servidor
Type	Necesario. El valor debe ser: normal, DB2z o IMS.

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

delete_quarantine_until

Utilizar en políticas.

Tabla 30. delete_quarantine_until

Parámetro	Descripción
quarantineUntil	Necesario.
dbUser	Necesario. Usuario de base de datos
serverIP	Necesario. IP de servidor
serverName	Necesario. Nombre de servidor
Type	Necesario. El valor debe ser: normal, DB2z o IMS.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

must_gather

Utilice el mandato must_gather para recopilar información sobre el estado del sistema Guardium que puede utilizar el servicio de soporte de Guardium. Consulte Información básica del soporte de IBM para obtener más información sobre este tema.

Tabla 31. must_gather

Parámetro	Descripción
commandsList	Serie - necesario
description	Serie - necesario
duration	Entero - necesario
emailDestination	Serie - necesario
invokingUser	Serie - necesario
maxLength	Entero - necesario
pmrNumber	Serie - necesario
start	Fecha - necesario
timestamp	Fecha - necesario
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

restart_job_queue_listener

Utilice el mandato restart_job_queue_listener para reiniciar el escucha de cola de trabajos si ésta no se puede iniciar o no ejecuta trabajos en espera, o si un trabajo parece estar bloqueado o está en estado detenido durante un periodo de tiempo prolongado. Si se emite este mandato inmediatamente se reinicia la cola de trabajos y se detienen y reinician todos los trabajos en ejecución.

Ejemplo:

```
grdapi restart_job_queue_listener
```

El mandato restart_job_queue_listener no acepta ningún parámetro.

update_quarantine_allowed_until

Utilizar en políticas.

Tabla 32. update_quarantine_allowed_until

Parámetro	Descripción
allowedUntil	Necesario.
dbUser	Necesario. Usuario de base de datos
serverIP	Necesario. IP de servidor
serverName	Necesario. Nombre de servidor
Type	Necesario. El valor debe ser: normal, DB2z o IMS.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

update_quarantine_until

Utilizar en políticas.

Tabla 33. update_quarantine_until

Parámetro	Descripción
quarantineUntil	Necesario.
dbUser	Necesario. Usuario de base de datos
serverIP	Necesario. IP de servidor
serverName	Necesario. Nombre de servidor
Type	Necesario. El valor debe ser: normal, DB2z o IMS.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Tema principal: Referencia de GuardAPI

Funciones de reescritura de consultas de GuardAPI

Automatice la realización o creación de pruebas o definiciones para determinadas consultas complejas que no se pueden realizar desde la interfaz de usuario utilizando las API de Guardium en la interfaz de línea de mandatos.

Nota: Si crea definiciones de reescritura de consulta utilizando las API, puede seguir utilizando la interfaz de usuario para recuperar esas definiciones y probarlas con el Creador de reescritura de consultas.

Las funciones de GuardAPI relacionadas con la reescritura de consultas son:

assign_qr_condition_to_action

create_qr_action

create_qr_add_where

create_qr_add_where_by_id

create_qr_condition

create_qr_definition

create_qr_replace_element

create_qr_replace_element_byId

list_qr_action

list_qr_add_where

list_qr_add_where_by_id

list_qr_condition

list_qr_condition_to_action

list_qr_definitions

list_qr_replace_element

list_qr_replace_element_byId

remove_all_qr_replace_elements

remove_all_qr_replace_elements_byId

remove_qr_action

remove_qr_add_where_by_id

remove_qr_condition

remove_qr_definition

remove_qr_replace_element_byId

update_qr_action

update_qr_add_where_by_id

update_qr_condition

update_qr_definition

update_qr_replace_element_byId

assign_qr_condition_to_action

Crear una asociación entre una condición de reescritura de consulta y una acción asociada.

Parámetro	Descripción
actionName	Necesario. El nombre de la acción de reescritura de consulta.
conditionName	Necesario. El nombre de la condición de reescritura de consulta que se va a asociar con la acción especificada.
definitionName	Necesario. El nombre de la condición de reescritura de consulta que se va a asociar con la condición y la acción especificadas.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

```
grdapi assign_qr_condition_to_action definitionName="case 15" actionName="qr action15_2" conditionName="qr cond15_2"
```

create_qr_action

Cree una acción de reescritura de consulta para una definición de reescritura de consulta especificada.

Parámetro	Descripción

Parámetro	Descripción
actionName	Necesario. El nombre exclusivo de la acción de reescritura de consulta.
definitionName	Necesario. La definición de reescritura de consulta que se va a asociar con esta acción.
description	Una descripción opcional.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

```
grdapi create_qr_action definitionName="case 15" actionName="qr action15_3"
```

create_qr_add_where

Asociar una función de reescritura de consulta para añadir una condición WHERE a la acción de reescritura de consulta especificada.

Parámetro	Descripción
actionName	Necesario. El nombre exclusivo de la acción de reescritura de consulta.
definitionName	Necesario. La definición de reescritura de consulta que se va a asociar con esta acción.
whereText	Texto para añadir a una cláusula WHERE.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi create_qr_add_where definitionName="qrw_def_Oracle_1" actionName="qrw_act__addwhere_id2" whereText="id=2"

create_qr_add_where_by_id

Asociar una función de reescritura de consulta para añadir una condición WHERE a la acción de reescritura de consulta especificada.

Parámetro	Descripción
qrActionId	Necesario (entero). El ID exclusivo de la acción de reescritura de consulta.
whereText	Texto para añadir a una cláusula WHERE.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi create_qr_add_where_by_id qrActionId=10002 whereText="id=2"

create_qr_condition

Crear una condición de reescritura de consulta.

Parámetro	Descripción
conditionName	Necesario. El nombre exclusivo de esta condición de reescritura de consulta.
definitionName	Necesario. La definición de reescritura de consulta que se va a asociar con esta condición.
depth	Un entero que especifica la profundidad del SQL analizado al que se aplica esta condición (1 y superior). El valor predeterminado -1 significa que la condición de reescritura de consulta se aplica a cualquier SQL coincidente en cualquier profundidad.
isForAllRuleObjects	True o false. Utilice este parámetro para asociar esta condición con objetos en una regla de acceso de política. True indica que la condición especificada se aplica a todos los objetos del campo Objeto o Grupo de objetos de una regla activada. El valor predeterminado es false, lo que significa que la condición de consulta se especifica utilizando los objetos definidos en esta condición. Ninguna de las opciones afecta a ningún comportamiento de desencadenamiento de reglas.
isForAllRuleVerbs	True o false. Utilice este parámetro para asociar esta condición con objetos en una regla de acceso de política. True indica que la condición especificada se aplica a todos los verbos del campo Verbo o Grupo de verbos de una regla activada. El valor predeterminado es false, lo que significa que la condición de consulta se especifica utilizando los verbos definidos en esta condición. Ninguna de las opciones afecta a ningún comportamiento de desencadenamiento de reglas.
isObjectRegex	True o false. Indica que el objeto especificado se especifica utilizando una expresión regular. El valor predeterminado es false.
isVerbRegex	True o false. Indica que el verbo especificado se especifica utilizando una expresión regular. El valor predeterminado es false.
object	Un objeto (tabla, vista). El valor predeterminado "*" significa todos los objetos. También se puede especificar como una expresión regular, en cuyo caso, establezca isVerbRegex en true.
order	Se utiliza para especificar el orden en el que se ensamblan varias condiciones de reescritura de consulta relacionadas en SQL complejo. El valor predeterminado es 1.
verb	Un verbo (select, insert, update, delete). El valor predeterminado "*" significa todos los verbos.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi create_qr_condition definitionName="case 15" conditionName="qr cond15_3" verb=select isForAllRuleObjects=false object=* depth=2 order=3

create_qr_definition

Crear una acción de reescritura de consulta.

Parámetro	Descripción
dataBaseType	Necesario. El tipo de base de datos con el que está asociada esta definición de reescritura de consulta. Los valores válidos son: ORACLE o DB2.
definitionName	Necesario. Un nombre exclusivo para esta condición de reescritura de consulta.
description	Una descripción opcional.
isNegateQrCond	Indica si hay un distintivo NOT en el conjunto de condiciones de reescritura de consulta asociadas a esta definición.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi create_qr_definition dataBaseType="ORACLE" definitionName="case 15"

create_qr_replace_element

Cree un elemento de sustitución, o un conjunto de elementos como, por ejemplo, una sentencia SQL completa o una lista SELECT.

Parámetro	Descripción
actionName	Necesario. El nombre exclusivo de la acción de reescritura de consulta asociada esta función de reescritura.

Parámetro	Descripción
definitionName	Necesario. Un nombre exclusivo para esta condición de reescritura de consulta.
isFromAllRuleElements	True o false. Indica que esta acción se aplica a todos los elementos FROM. El valor predeterminado es false.
isFromRegex	True o false. Indica que el elemento "from" se especifica utilizando una expresión regular. El valor predeterminado es false.
isReplaceToFunction	True o false. Indica que "replace to" es el nombre de una función, tal como una función definida por el usuario.
replaceFrom	La serie de entrada para una regla coincidente que se va a sustituir. Utilice replaceType para indicar específicamente qué elemento de la consulta entrante se ha de examinar.
replaceTo	La serie de sustitución para el elemento coincidente.
replaceType	Necesario. Indica lo que se va a sustituir. Debe ser uno de los siguientes: • SELECT • VERB • OBJECT • SENTENCE • SELECTLIST
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi create_qr_replace_element definitionName="case 15" actionName="qr action15_2" replaceType=VERB replaceFrom="select" replaceTo="select++"

create_qr_replace_element_byId

Crear una especificación de sustitución para una acción de reescritura de consulta especificada.

Parámetro	Descripción
isFromAllRuleElements	True o false. Indica que esta acción se aplica a todos los elementos FROM. El valor predeterminado es false.
isFromRegex	True o false. Indica que el elemento "from" se especifica utilizando una expresión regular. El valor predeterminado es false.
isReplaceToFunction	True o false. Indica que "replace to" es el nombre de una función, tal como una función definida por el usuario.
qrActionId	Necesario (entero). El ID exclusivo de la acción de reescritura de consulta.
replaceFrom	La serie de entrada para una regla coincidente que se va a sustituir. Utilice replaceType para indicar específicamente qué elemento de la consulta entrante se ha de examinar.
replaceTo	La serie de sustitución para el elemento coincidente.
replaceType	Necesario. Indica lo que se va a sustituir. Debe ser uno de los siguientes: • SELECT • VERB • OBJECT • SENTENCE • SELECTLIST
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi create_qr_replace_element_byId qrActionID="1116" replaceType=OBJECT replaceFrom="employee" replaceTo="employee_2"

list_qr_action

Lista las acciones de consulta para una definición de consulta especificada.

Parámetro	Descripción
actionName	El nombre de la acción de reescritura de consulta.
definitionName	Necesario. El nombre de la definición de reescritura de consulta.
detail	True o false. El valor predeterminado es true, que lista todos los atributos asociados de las acciones. Si es false, solo se devuelve el nombre.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi list_qr_action definitionName="case 2"

Salida:

```
qrwg1.guard.swg.usma.ibm.com> grdapi list_qr_action definitionName="case 2"
########################################################################


         QR actions of definition 'case 2' - (id = 1 )

########################################################################
qr action ID: 1
qr action name: qr action2
qr action description: add where by id

ok
Example:
grdapi list_qr_action definitionName="case 2" detail=false

Output:

qrwg1.guard.swg.usma.ibm.com> grdapi list_qr_action definitionName="case 2" detail=false
################################
         QR actions of definition 'case 2' - (id = 1 )
################################
qr action2
ok
```

list_qr_add_where

Lista las funciones "add where" para un par de acción de consulta y definición de consulta que se ha especificado.

Parámetro	Descripción
actionName	El nombre de la acción de reescritura de consulta.
definitionName	Necesario. El nombre de la definición de reescritura de consulta.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi list_qr_add_where actionName="qrw_act_addwhere_id2" definitionName="qrw_def_Oracle_1"

list_qr_add_where_by_id

Lista las funciones "add where" para una acción de consulta especificada.

Parámetro	Descripción
qrActionId	Necesario (entero). El identificador exclusivo de la acción de reescritura de consulta.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi list_qr_add_where_by_id qrActionId=20023

list_qr_condition

Lista las condiciones de reescritura asociadas a una definición de reescritura de consulta determinada.

Parámetro	Descripción
conditionName	El nombre de una condición de reescritura de consulta.
definitionName	Necesario. Una definición de reescritura de consulta.
detail	True o false. El valor predeterminado es true, que lista todos los atributos asociados de las condiciones. Si es false, solo se devuelve el nombre.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi list_qr_condition definitionName="case 2" conditionName="qr cond2"

Salida:

```
qrwg1.guard.swg.usma.ibm.com> grdapi list_qr_condition definitionName="case 2" conditionName="qr cond2"
######################################################################
         QR Condtions of Definition 'case 2' - (id = 1 )

######################################################################

qr condition id: 1
qr condition name: qr cond2
qr definition ID: 1
qr condition verb: *
qr condition object: *
qr condition dept: -1
is verb regex: false
is object regex: false
is action for all rule verbs: false
is action for all rule objects: false
qr condition order: 1
```

list_qr_condition_to_action

Lista las asociaciones entre una condición de reescritura de consulta y una acción de reescritura de consulta para una definición de consulta determinada.

Parámetro	Descripción
actionName	Necesario (entero). El identificador exclusivo de la acción de reescritura de consulta.
definitionName	Necesario. Una definición de reescritura de consulta.
Detail	True o false. El valor predeterminado es true, que lista todos los atributos asociados de las condiciones para la acción y definición especificadas. Si es false, solo se devuelve el nombre.

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi list_qr_condition_to_action actionName="qr action15_2" definitionName="case 15"

Salida:

```
qrwg1.guard.swg.usma.ibm.com> grdapi list_qr_condition_to_action actionName="qr action2" definitionName="case 2"
######################################################################

         QR Condtions of Action 'qr action2' - (id = 1 )

######################################################################

qr condition id: 1
qr condition name: qr cond2
qr definition ID: 1
qr condition verb: *
qr condition object: *
qr condition dept: -1
is verb regex: false
is object regex: false
is action for all rule verbs: false
is action for all rule objects: false
qr condition order: 1
```

list_qr_definitions

Lista las definiciones de reescritura de consulta.

Parámetro	Descripción
definitionName	Necesario. Una definición de reescritura de consulta.
Detail	True o false. El valor predeterminado es true, que lista todos los atributos asociados de las condiciones para la acción y definición especificadas. Si es false, solo se devuelve el nombre.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi list_qr_definitions

Salida:

```
qrwg1.guard.swg.usma.ibm.com> grdapi list_qr_definitions
######################################################################
         QR  Definitions

######################################################################
qr definition ID: 1
qr definition name: case 2
qr definition description:
is negation set on qr conditions: false
```

list_qr_replace_element

Lista las sustituciones para un par de acción de reescritura de consulta y definición de reescritura de consulta especificadas.

Parámetro	Descripción

Parámetro	Descripción
actionName	Necesario. Una acción de reescritura de consulta.
definitionName	Necesario. Una definición de reescritura de consulta.
Detail	True o false. El valor predeterminado es true, que lista todos los atributos asociados de los elementos de sustitución para la acción y definición especificadas. Si es false, solo se devuelven nombres.
replaceType	Si se especifica, debe ser uno de los siguientes: • SELECT • VERB • OBJECT • SENTENCE • SELECTLIST
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi list_qr_replace_element actionName="qr action2" definitionName="case 2"

Salida:

```
qrwg1.guard.swg.usma.ibm.com> grdapi list_qr_replace_element actionName="qr action2" definitionName="case 2"
########################################################################
         QR replace elements for action 'qr action2' - (qrActionId = 1 )

########################################################################

qr replace element ID: 1
qr replace type: object
qr replace from: emp
qr replace to: NEW_EMP
qr is from regex: false
qr is from all rule elements: false

************************************************************************
qr replace element ID: 2
qr replace type: selectList
qr replace from: Whole select list
qr replace to: EMPNO,SAL
qr is from regex: false
qr is from all rule elements: false
```

list_qr_replace_element_byId

Lista las sustituciones para una acción de reescritura de consulta especificada.

Parámetro	Descripción
detail	True o false. El valor predeterminado es true, que lista todos los atributos asociados de los elementos de sustitución para la acción y definición especificadas. Si es false, solo se devuelven nombres.
qrActionId	Necesario (entero). El identificador exclusivo de la acción de reescritura de consulta.
replaceType	Si se especifica, debe ser uno de los siguientes: • SELECT • VERB • OBJECT • SENTENCE • SELECTLIST

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi list_qr_replace_element_byId detail=true qrActionId="22222" replaceType="OBJECT"

remove_all_qr_replace_elements

Suprime las especificaciones de sustitución de consulta del sistema.

Parámetro	Descripción
actionName	Necesario. Una acción de reescritura de consulta.
definitionName	Necesario (entero). El identificador exclusivo de la acción de reescritura de consulta.
replaceType	Si se especifica, debe ser uno de los siguientes: • SELECT • VERB • OBJECT • SENTENCE • SELECTLIST
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi remove_all_qr_replace_elements definitionName="new case 2" actionName="new qr action2“

remove_all_qr_replace_elements_byId

Suprime las especificaciones de sustitución de consulta del sistema.

Parámetro	Descripción
qrActionId	Necesario (entero). Un identificador de acción de reescritura de consulta.
definitionName	Necesario. Una definición de reescritura de consulta.
replaceType	Si se especifica, debe ser uno de los siguientes: • SELECT • VERB • OBJECT • SENTENCE • SELECTLIST Si no se especifica replaceType, se suprimen todas las sustituciones para la acción y la definición especificadas.

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi remove_all_qr_replace_elements actionName="qr action15_2" definitionName="case 15" replaceType="OBJECT"

remove_qr_action

Suprime una acción de reescritura de consulta especificada del sistema.

Parámetro	Descripción
actionName	Necesario. Una acción de reescritura de consulta.
definitionName	Necesario. Una definición de reescritura de consulta.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi remove_qr_action actionName="qr action15_2" definitionName="case 15"

remove_qr_add_where_by_id

Suprime una función "add where" especificada del sistema.

Parámetro	Descripción
qrAddWhereId	Necesario (entero). Una función "add where".
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi remove_qr_add_where_by_id qrAddWhereId=22666

remove_qr_condition

Suprime una condición de reescritura de consulta del sistema.

Parámetro	Descripción
conditionName	Necesario. Una condición de reescritura de consulta.
definitionName	Necesario. Una definición de reescritura de consulta.

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi remove_qr_condition conditionName="qr cond15_1" definitionName="case 15"

remove_qr_definition

Suprime una definición de reescritura de consulta del sistema.

Parámetro	Descripción
definitionName	Necesario. Una definición de reescritura de consulta.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi remove_qr_definition definitionName="case 15"

remove_qr_replace_element_byId

Suprime una sustitución de elemento de consulta especificado del sistema.

Parámetro	Descripción
qrReplaceElementId	Necesario (entero). Un ID de definición de sustitución.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi qrReplaceElementId=33333

update_qr_action

Actualiza una acción de reescritura de consulta existente con un nombre nuevo y una descripción opcional.

Parámetro	Descripción
actionName	Necesario. El nombre exclusivo de la acción de reescritura de consulta.
definitionName	Necesario. La definición de reescritura de consulta que se va a asociar con esta acción.
description	Una descripción opcional.
newName	El nuevo nombre de la acción de reescritura de consulta.

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi update_qr_action definitionName="case 2" actionName="qr action2" newName="new qr action2"

update_qr_add_where_by_id

Permite actualizar una función "add where" existente con un nuevo texto de sustitución.

Parámetro	Descripción
qrAddWhereId	Necesario (entero). El identificador exclusivo de la función "add where" de reescritura de consulta.
whereText	El texto de sustitución para la cláusula where identificada.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi update_qr_add_where_by_id 22222 whereText="1=2"

update_qr_condition

Actualizar una condición de reescritura de consulta existente.

Parámetro	Descripción
conditionName	Necesario. El nombre exclusivo de esta condición de reescritura de consulta.
definitionName	Necesario. La definición de reescritura de consulta que se va a asociar con esta condición.
depth	Un entero que especifica la profundidad del SQL analizado al que se aplica esta condición (1 y superior). El valor predeterminado -1 significa que la condición de reescritura de consulta se aplica a cualquier SQL coincidente en cualquier profundidad.
isForAllRuleObjects	True o false. Indica que la condición especificada se aplica a todos los objetos para la regla activada. El valor predeterminado es false.
isForAllRuleVerbs	True o false. Indica que la condición especificada se aplica a todos los verbos para la regla activada. El valor predeterminado es false.
isObjectRegex	True o false. Indica que el objeto especificado se especifica utilizando una expresión regular. El valor predeterminado es false.
isVerbRegex	True o false. Indica que el verbo especificado se especifica utilizando una expresión regular. El valor predeterminado es false.
newName	El nuevo nombre de la condición de reescritura de consulta.
Object	Un objeto (tabla o vista). El valor predeterminado "*" significa todos los objetos. También se puede especificar como una expresión regular, en cuyo caso, establezca isVerbRegex en true.
Order	Se utiliza para especificar el orden en el que se ensamblan varias condiciones de reescritura de consulta relacionadas en SQL complejo. El valor predeterminado es 1.
Verb	Un verbo (select, insert, update, delete). El valor predeterminado "*" significa todos los verbos.

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

grdapi update_qr_condition definitionName="case 16" conditionName="qr cond15_3" newName="qr cond16_3" verb=select object=* dept=2 order=3

update_qr_definition

Actualizar una definición de reescritura de consulta existente.

Parámetro	Descripción
dataBaseType	Necesario. El tipo de base de datos con el que está asociada esta definición de reescritura de consulta. Debe ser ORACLE o DB2.
definitionName	Necesario. Un nombre exclusivo para esta condición de reescritura de consulta.
description	Una descripción opcional.
isNegateQrCond	Indica si hay un distintivo NOT en el conjunto de condiciones de reescritura de consulta asociadas a esta definición.
newName	Opcional. Especifique un nombre nuevo exclusivo.
sampleSql	Opcional. Especifique una sentencia SQL de ejemplo. En la mayoría de los casos no se utiliza, a menos que posteriormente desee utilizar el SQL de ejemplo de entrada en la interfaz de usuario.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

```
grdapi update_qr_definition dataBaseType="DB2" definitionName="case 15" sampleSql="select EMPNO from EMP where ENAME = (select
ENAME from EMP where SAL = (select SAL from EMP where HIREDATE = to_date('06/09/1981 00:00:00', 'MM/DD/YYYY HH24:MI:SS')))"
newName="DB2_case 15"
```

update_qr_replace_element_byId

Actualizar una especificación de sustitución para una acción de reescritura de consulta especificada.

Parámetro	Descripción
isFromAllRuleElements	Necesario. El tipo de base de datos con el que está asociada esta definición de reescritura de consulta. Debe ser ORACLE o DB2.
isFromRegex	True o false. Indica que el elemento "from" se especifica utilizando una expresión regular. El valor predeterminado es false.
isReplaceToFunction	True o false. Indica que "replace to" es el nombre de una función, tal como una función definida por el usuario.
qrReplaceElementId	Necesario (entero). El ID exclusivo de la acción de reescritura de consulta.
replaceFrom	La serie de entrada para una regla coincidente que se va a sustituir. Utilice replaceType para indicar específicamente qué elemento de la consulta entrante se ha de examinar.
replaceTo	La serie de sustitución para el elemento coincidente.

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

```
grdapi update_qr_replace_element_byId qrReplaceElementId=1 isFromAllRuleElements=false isFromRegex=false isReplaceToFunction=false
replaceFrom=emp replaceTo=NEW_EMP_UPDATED
```

Tema principal: Referencia de GuardAPI

Funciones de rol de GuardAPI

Utilice estos mandatos de GuardAPI para otorgar, listar y revocar funciones de roles.

Nota: En un entorno de gestión Central, el objeto al que desea añadir un rol puede residir en el Gestor central o en una unidad gestionada. Consulte la publicación de ayuda Agregación y gestión central, para obtener más información.

grant_role_to_object_by_id

Añadir un rol al objeto especificado, por ejemplo, un proceso de clasificación. Las dependencias se comprueban antes de añadir el rol. Por ejemplo, antes de añadir un rol a un proceso de Clasificación, dicho rol debe asignarse a todos los componentes incluidos en dicho proceso de clasificación (la política de clasificación y cualquier origen de datos al que se haga referencia).

Tabla 1. grant_role_to_object_by_id

Parámetro	Descripción
objectTypeId	Necesario (entero). Identifica el tipo de objeto al que se asignará el rol. Debe ser uno de los enteros siguientes: 1=Query 2=Report 3=Alert 4=Baseline 5=Policy 6=SecurityAssessment 7=PrivacySet 8=AuditProcess 12=CustomTable 13=Datasource 14=CustomDomain 15=ClassifierPolicy 16=ClassificationProcess
objectId	Necesario (entero). Identifica el objeto al que se asignará el rol.
roleId	Necesario (entero). Identifica el rol que se va asignar. Puede ser cualquier ID de rol existente, o el valor especial -1, que permite el acceso para todos los roles.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

grdapi grant_role_to_object_by_id objectTypeId=13 objectId=2 roleId=3

grant_role_to_object_by_Name

Añadir un rol al objeto especificado, por ejemplo, un proceso de clasificación. Las dependencias se comprueban antes de añadir el rol. Por ejemplo, antes de añadir un rol a un proceso de Clasificación, dicho rol debe asignarse a todos los componentes contenidos en dicho proceso de clasificación (la política de clasificación y los orígenes de datos referenciados). Parámetros

Tabla 2. grant_role_to_object_by_Name

Parámetro	Descripción
objectType	Necesario. Identifica el tipo de objeto al que se asignará el rol. Debe ser uno de los valores siguientes: Query Report Alert Baseline Policy SecurityAssessment PrivacySet AuditProcess CustomTable Datasource CustomDomain ClassifierPolicy ClassificationProcess
objectName	Necesario. El nombre del objeto, por ejemplo, la consulta o el informe al que se asignará el rol.
role	Necesario. El nombre del rol que se ha de asignar. Puede ser cualquier rol existente, o **all_roles** para permitir el acceso a todos los roles.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

grdapi grant_role_to_object_by_Name objectType=Datasource objectName= “swanSybase” role=admin

list_roles_granted_to_object_by_id

Muestra los roles asignados al objeto especificado, Por ejemplo, un proceso de clasificación.

Tabla 3. list_roles_granted_to_object_by_id

Parámetro	Descripción

Parámetro	Descripción
objectTypeId	Necesario (entero). Identifica el tipo de objeto al que se asignará el rol. Debe ser uno de los enteros siguientes: 1=Query 2=Report 3=Alert 4=Baseline 5=Policy 6=SecurityAssessment 7=PrivacySet 8=AuditProcess 12=CustomTable 13=Datasource 14=CustomDomain 15=ClassifierPolicy 16=ClassificationProcess
objectId	Necesario (entero). Identifica el objeto al que se asignará el rol.
roleId	Necesario (entero). Identifica el rol que se va asignar. Puede ser cualquier ID de rol existente, o el valor especial -1, que permite el acceso para todos los roles.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

grdapi list_roles_granted_to_object_by_id objectTypeId=7 objectId=1

list_roles_granted_to_object_by_Name

Muestra los roles asignados al objeto especificado, Por ejemplo, un proceso de clasificación.

Tabla 4. list_roles_granted_to_object_by_Name

Parámetro	Descripción
objectType	Necesario. Identifica el tipo de objeto al que se asignará el rol. Debe ser uno de los valores siguientes: Query Report Alert Baseline Policy SecurityAssessment PrivacySet AuditProcess CustomTable Datasource CustomDomain ClassifierPolicy ClassificationProcess

Parámetro	Descripción
objectName	Necesario. El nombre del objeto, por ejemplo, la consulta o el informe al que se asignará el rol.
role	Necesario. El nombre del rol que se ha de asignar. Puede ser cualquier rol existente, o **all_roles** para permitir el acceso a todos los roles.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

grdapi list_roles_granted_to_object_by_Name objectType=PrivacySet objectName="privaceSet 1"

revoke_role_from_object_by_id

Elimina un rol del objeto especificado, por ejemplo, un proceso de clasificación. Las dependencias se manejan automáticamente. Por ejemplo si se elimina el rol foo de una consulta especificada, también se elimina el rol foo de cualquier informe basado en dicha consulta.

Tabla 5. revoke_role_from_object_by_id

Parámetro	Descripción
objectTypeId	Necesario (entero). Identifica el tipo de objeto al que se asignará el rol. Debe ser uno de los enteros siguientes: 1=Query 2=Report 3=Alert 4=Baseline 5=Policy 6=SecurityAssessment 7=PrivacySet 8=AuditProcess 12=CustomTable 13=Datasource 14=CustomDomain 15=ClassifierPolicy 16=ClassificationProcess
objectId	Necesario (entero). Identifica el objeto al que se asignará el rol.
roleId	Necesario (entero). Identifica el rol que se va asignar. Puede ser cualquier ID de rol existente, o el valor especial -1, que permite el acceso para todos los roles.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

grdapi revoke_role_from_object_by_id objectTypeId=13 objectId=5 role=-1

revoke_role_from_object_by_Name

Elimina un rol del objeto especificado, por ejemplo, un proceso de clasificación. Las dependencias se manejan automáticamente. Por ejemplo si se elimina el rol foo de una consulta especificada, también se elimina el rol foo de cualquier informe que utiliza dicha consulta.

Tabla 6. revoke_role_from_object_by_Name

Parámetro	Descripción
objectType	Necesario. Identifica el tipo de objeto al que se asignará el rol. Debe ser uno de los valores siguientes: Query Report Alert Baseline Policy SecurityAssessment PrivacySet AuditProcess CustomTable Datasource CustomDomain ClassifierPolicy ClassificationProcess
objectName	Necesario. El nombre del objeto, por ejemplo, la consulta o el informe al que se asignará el rol.
role	Necesario. El nombre del rol que se ha de asignar. Puede ser cualquier rol existente, o **all_roles** para permitir el acceso a todos los roles.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

grdapi revoke_role_from_object_by_Name objectType=Datasource objectName="swanSybase" role=admin

Tema principal: Referencia de GuardAPI

Funciones de GuardAPI S-TAP

Utilice estos mandatos de CLI para crear, listar, suprimir, reiniciar y establecer funciones de S-TAP.

create_stap_inspection_engine

Añadir un motor de inspección al S-TAP especificado. Las configuraciones de S-TAP solo se pueden modificar desde el host Guardium activo para dicho S-TAP, y solo cuando S-TAP está en línea.

Tabla 1. create_stap_inspection_engine

Parámetro	Descripción
stapHost	Necesario. El nombre de host o la dirección IP del servidor de bases de datos en el que está instalado S-TAP.

Parámetro	Descripción
protocol	Necesario. El protocolo de base de datos, que debe ser uno de estos valores: DB2 DB2 Exit (DB2 versión 10) FTP Informix Kerberos Mysql Netezza Oracle PostgreSQL Sybase Teradata Windows File Share excluir IE Los hosts WindowsS-TAP también pueden utilizar los protocolos siguientes: MSSQL conexiones con nombre
portMin	Necesario (entero). Número de puerto inicial del rango de puertos de escucha que se han configurado para la base de datos. (No utilice rangos inclusivos grandes, ya que degrada el rendimiento de S-TAP).
portMax	Necesario (entero). Número de puerto final del rango de puertos de escucha para la base de datos.
teeListenPort teeRealPort	Opcional (entero). No se utiliza para Windows. En UNIX, se sustituye por el puerto real de BD de KTAP, cuando se utiliza el mecanismo de supervisión de K-TAP. Es obligatorio cuando se utiliza el mecanismo de supervisión de TEE. El puerto de escucha es el puerto en el que S-TAP escucha y acepta el tráfico de la base de datos local. El puerto real es el puerto en que S-TAP reenvía el tráfico.
connectToIp	Opcional (entero). La dirección IP de S-TAP que se utilizará para conectar con la base de datos. Algunas bases de datos aceptan la conexión local solo en la dirección IP "real" de la máquina y no en el valor predeterminado (127.0.0.1).
client	Necesario. Una lista de direcciones IP de cliente y máscaras correspondientes para especificar qué clientes se deben supervisar. Si la dirección IP es la misma que la dirección IP para el servidor de bases de datos, y se utiliza una máscara de 255.255.255.255, solo se supervisa el tráfico local. Un valor de dirección/máscara de cliente de 1.1.1.1/0.0.0.0 supervisa todos los clientes. (Consulte el ejemplo).
encryption	Opcional. Activar el tráfico cifrado ASO, donde encryption=0 (no) o encryption=1 (sí).
excludeClient	Opcional. Una lista de direcciones IP de cliente y máscaras correspondientes para especificar qué clientes se deben excluir. Esta opción le permite configurar S-TAP para que supervise todos los clientes, excepto un determinado cliente o subred (o un grupo de estas opciones).
procNames	En un servidor de Windows: Solo para Oracle o MS SQL Server, cuando se utilizan conexiones con nombre. En Oracle, la lista normalmente tiene dos entradas: oracle.exe, tnslsnr.exe. En MS SQL Server, la lista suele ser solo una entrada: sqlservr.exe.
namedPipe	Solo Windows. Especifica el nombre de un conducto con nombre. Si se utiliza un conducto con nombre, pero no se especifica nada aquí, S-TAP recupera el nombre de conducto con nombre del registro.
ktapDbPort	Opcional (entero). No se utiliza para Windows. En UNIX, se utiliza solo cuando se utiliza el mecanismo de supervisión de K-TAP. Identifica el puerto de base de datos que debe supervisar el mecanismo de K-TAP.
dbInstallDir	Solo para UNIX. Escriba el nombre completo de vía de acceso del directorio de instalación de la base de datos. Por ejemplo: /home/oracle10
procName	Para un servidor UNIX: Para una base de datos DB2, Oracle o Informix, especifique el nombre completo de vía de acceso al ejecutable de la base de datos. Por ejemplo: /home/oracle10/prod/10.2.0/db_1/bin/oracle
procNames	Opcional
db2SharedMemAdjustment db2SharedMemClientPosition db2SharedMemSize	Estos tres parámetros se utilizan para un motor de inspección de DB2, sólo bajo las condiciones siguientes: • El servidor DB2 se está ejecutando en Linux. • El mecanismo de supervisión de K-TAP está instalado. • Los clientes se conectan a DB2 utilizando la memoria compartida. Cuando se utilizan estos parámetros, grdapi solo verifica que el protocolo sea db2, no verifica que se cumplan las condiciones. Consulte el tema DB2Linux S-TAP, para obtener una explicación detallada de cómo utilizar estos parámetros.

Parámetro	Descripción
instanceName	Opcional (cadena). Solo se utiliza para el tráfico cifrado de MSSQL o de Oracle. Debe activarse el distintivo de cifrado de MSSQL u ORACLE para poder utilizar este parámetro.
informixVersion	Versión de Informix.
ieIdentifier	Opcional (cadena).
interceptTypes	Opcional (cadena).
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi create_stap_inspection_engine stapHost=192.168.2.118 protocol=Oracle portMin=1521 portMax=1521 dbInstallDir=/data/oracle10
procName=/data/oracle10/oracle/product/10.2.0/db_1/bin/oracle client=192.168.0.0/255.255.0.0 ktapDbPort=1521
```

Nota:

Algunas veces, cuando se añade un motor de inspección, se visualiza un mensaje falso acerca de que se S-TAP ha rechazado la configuración y debe consultar el registro de sucesos S-TAP, a pesar de que la configuración no se ha rechazado y se ha instalado correctamente.

La IP/máscara de cliente es necesaria para UNIXS-TAP y opcional para WindowsS-TAP.

list_inspection_engines

Mostrar las propiedades de todos los S-TAP en el host especificado, opcionalmente solo para un tipo de base de datos específico.

Tabla 2. list_inspection_engines

Parámetro	Descripción
stapHost	Necesario. El nombre de host o la dirección IP de un servidor de bases de datos en el que se instalan los S-TAP (y se configuran para enviar informes a este dispositivo Guardium).
type	Opcional. Si se utiliza, solo se listan los motores de inspección para el tipo de base de datos especificado. El tipo debe ser uno de los siguientes: db2 informix mssql mssql-np oracle sybase
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

a1.corp.com> grdapi list_inspection_engines stapHost=192.168.2.33 type=oracle

ID=20162

Stap Host: 192.168.2.33 - Not Active

oracle Inspection Engines:

name =ORACLE2

type =ORACLE

connect to IP=127.0.0.1

install dir = /home/oracle10

exec file = /home/oracle10/product/10.2.0/db_1/bin/oracle-guard

instance name = MSSQLSERVER

encrypted = no

port range = 1521 - 1521

tee listen port = null, tee rel port = 1521

client = 127.0.0.1/255.255.255.255

client = 192.168.0.0/255.255.0.0

name =ORACLE3

type =ORACLE

connect to IP=127.0.0.1

install dir = /home/oracle9

exec file = /home/oracle9/bin/oracle

instance name = MSSQLSERVER

encrypted = no

port range = 1521 - 1521

ok

list_staps

Visualizar los servidores de bases de datos desde los que informan los S-TAP a este sistema Guardium, opcionalmente listando solo los servidores que tienen S-TAP para los que este sistema Guardium es el host activo (es decir, el sistema al que S-TAP está enviando datos y desde el que se puede modificar la configuración de S-TAP).

Tabla 3. list_staps

Parámetro	Descripción
onlyActive	Opcional (booleano). Escriba **true**, u omita este parámetro, para listar solo los hosts que tengan S-TAP para los que este sistema Guardium es el host activo. Especifique **false** para listar todos los hosts en los que se han configurado los S-TAP para que utilicen este sistema Guardium como host primario o secundario.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

a1.corp.com> grdapi list_staps onlyActive=false

ID=0

staps:

stap host = FALCON

stap host = 192.168.2.33

stap host = 192.168.2.173

stap host = 192.168.2.248

stap host = jumbo

ok

delete_stap_inspection_engine

Eliminar un motor de inspección de S-TAP. Este sistema Guardium debe ser el host activo para el S-TAP desde el que se eliminará el motor de inspección.

Tabla 4. delete_stap_inspection_engine

Parámetro	Descripción
stapHost	Necesario. El nombre de host o la dirección IP del servidor de bases de datos en el que está instalado S-TAP.
type	Necesario. Identifica el tipo de inspección que se va a eliminar. El tipo debe ser uno de los siguientes: Cassandra, CouchDB, DB2, DB2 Exit, FTP, GreenPlumDB, Hadoop, HTTP, iSERIES, Informix, KERBEROS, MongoDB, MS SQL, mssql-np, Mysql, Named Pipes, Netezza, Oracle, PostgreSQL, SAP Hana, Sybase, Teradata, or Windows File Share
sequence	Necesario (entero). El número de secuencia del motor de inspección que se va a eliminar del conjunto de motores de inspección del tipo especificado. Puede utilizar primero el mandato grdapi list_inspection_engines con la opción type en primer lugar, para verificar el número de secuencia del motor de inspección que se va a eliminar.
waitForResponse	Opcional. Especifica si la API espera una respuesta de S-TAP. Los valores válidos son 0 (no esperar) y 1 (esperar una respuesta). El valor predeterminado es 1 cuando stapHost es un solo nombre de host o dirección IP y 0 en todos los demás casos.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi delete_stap_inspection_engine stapHost=192.168.2.118 type=Oracle sequence=1
```

Nota: A veces, si se suprime un motor de inspección, se muestra un mensaje falso que indica que no puede eliminar el motor de inspección o que no se ha encontrado el motor de inspección especificado, a pesar de que se ha eliminado correctamente.

restart_stap

Reiniciar un motor de inspección de S-TAP.

Tabla 5. restart_stap

Parámetro	Descripción
stapHost	Necesario. El nombre de host o la dirección IP del servidor de bases de datos en el que está instalado S-TAP.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi restart_stap stapHost=192.168.2.118
```

set_stap_debug

Filtrar el contenido del registro por base de datos, protocolo, información de cliente, en lugar de volcar todo el tráfico en el registro.

parámetros de función:

stapDebugInterval - necesario

stapDebugLevel - necesario

stapDebugOn - necesario

stapHost - necesario

api_target_host

store_stap_approval

Utilice esta función para impedir que los S-TAP no autorizados se conecten al sistema Guardium.

Si el valor es ON, los S-TAP no se pueden conectar hasta que se aprueben específicamente.

Si un S-TAP se desconectará inmediatamente hasta que lo autorice específicamente la dirección IP de dicho S-TAP.

Hay un informe predefinido para clientes aprobados y clientes TAP aprobados. Está disponible en el separador Supervisor diario.

Nota:

Se necesita una dirección IP válida, no el nombre de host.

El mandato store_stap_approval no funciona en un entorno en el que hay un equilibrador de carga de IP.

En un entorno gestionado central, después de añadir las direcciones IP a los STAP aprobados, hay un tiempo de espera asociado a la sincronización que puede durar hasta una hora. Una vez finalizada la sincronización, el estado del S-TAP aprobado aparecerá en verde en la GUI.

Función: store_stap_approval

parámetros de función:

isNeeded - booleano - necesario

api_target_host - Serie

Sintaxis

grdapi store_stap_approval ON | OFF

Mandato de CLI

store stap approval y show stap approval

add_approved_stap_client

Utilice este mandato de GuardAPI para añadir un cliente aprobado de S-TAP.

El uso de este mandato de GuardAPI no reinicia el sniffer y no afecta a los S-TAP ya conectados. Este mandato solo afecta a las conexiones nuevas del S-TAP.

Función: add_approved_stap_client

parámetros de función:

stapHost - Serie - necesario

api_target_host - Serie

Sintaxis

grdapi add_approved_stap_client <stapHost>

list_approved_stap_client

Utilice este mandato de GuardAPI para listar clientes aprobados de S-TAP.

Función: add_approved_stap_client

parámetros de función:

api_target_host - Serie

Sintaxis

grdapi list_approved_stap_client

list_stap_verification_results

Utilice este mandato de GuardAPI para los resultados de la verificación de S-TAP.

parámetros de función:

stapHost - cadena. El nombre de host o la dirección IP del servidor de bases de datos en el que está instalado S-TAP.

Sintaxis

grdapi list_stap_verification_results <stapHost>

delete_approved_stap_client

Utilice este mandato de GuardAPI para eliminar un cliente aprobado de S-TAP.

El uso de este mandato de GuardAPI no reinicia el sniffer y no afecta a los S-TAP que ya están conectados. Este mandato solo afecta a las conexiones de S-TAP.

Función: add_approved_stap_client

parámetros de función:

stapHost - Serie - necesario

api_target_host - Serie

Sintaxis

grdapi delete_approved_stap_client <stapHost - serie - necesario>

set_ktap_debug

ID=0

parámetros de función:

ktapDebugInterval - necesario

ktapFunctionNames

stapHost - necesario

api_target_host

display_stap_config

Mostrar las propiedades de todos los S-TAP del host especificado.

Tabla 6. display_stap_config

Parámetro	Descripción
stapHost	Necesario. El nombre de host o la dirección IP de un servidor de bases de datos en el que se han instalado y configurado los S-TAP para informar a este sistema Guardium, o una lista separada por comas de nombres de host o direcciones IP. También puede utilizar estos valores: all_active Todos los S-TAP configurados para informar a este sistema Guardium all_windows_active Todos los S-TAP configurados para informar a este sistema Guardium y que se ejecutan en máquinas Windows all_unix_active Todos los S-TAP configurados para informar a este sistema Guardium y que se ejecutan en máquinas UNIX

Ejemplos:

```
grdapi display_stap_config stapHost=myhost1,myhost2
grdapi display_stap_config stapHost=all_active
```

update_stap_config

Actualizar las propiedades de todos los S-TAP del host especificado.

Tabla 7. update_stap_config

Parámetro	Descripción
stapHost	Necesario. El nombre de host o la dirección IP de un servidor de bases de datos en el que está el sistema Guardium, o una lista separada por comas de nombres de host o direcciones IP. También puede utilizar estos valores: all_active Todos los S-TAP configurados para informar a este sistema Guardium all_windows_active Todos los S-TAP configurados para informar a este sistema Guardium y que se ejecutan en máquinas Windows all_unix_active Todos los S-TAP configurados para informar a este sistema Guardium y que se ejecutan en máquinas UNIX
updateValue	Necesario. Uno o varios pares de clave-valor, con ese formato: *section.nombre_parámetro:nuevo_valor*. *section* indica la sección del archivo guard_tap.ini que contiene el parámetro; puede ser TAP o DB_x, donde DB_x es una designación para un motor de inspección que se muestra como una cabecera de sección en el archivo. Puede especificar valores nuevos para varios parámetros separando las entradas con un ampersand (&).
waitForResponse	Opcional. Especifica si la API esperará una respuesta de S-TAP. Los valores válidos son 0 (no esperar) y 1 (esperar una respuesta). El valor predeterminado es 1 cuando stapHost es un solo nombre de host o dirección IP y 0 en todos los demás casos.

Ejemplos:

```
grdapi update_stap_config stapHost=all_windows_active updateValue=TAP.XXXX
```

verify_stap_inspection_engine_with_sequence

Utilice este mandato para verificar el motor de inspección de S-TAP.

parámetros de función:

addToSchedule - Serie - Lista de valores de constantes; los valores válidos son Yes y No.

datasourceName - Serie. Si se especifica este parámetro, se realiza una verificación avanzada en el origen de datos especificado. Si se omite este parámetro, se realiza la verificación estándar.

sequence - Entero - necesario. El número de secuencia del motor de inspección existente para su verificación. Puede utilizar primero el mandato grdapi list_inspection_engines con la opción type en primer lugar, para comprobar el número de secuencia del motor de inspección que se va a verificar.

stapHost - Serie - necesario - El nombre de host o la dirección IP del servidor de bases de datos en el que está instalado S-TAP.

protocol - Necesario. El protocolo de base de datos, que puede ser uno de estos valores: DB2, DB2 Exit (DB2 versión 10), FTP, Informix, Kerberos, Mysql, Netezza, Oracle, PostgreSQL, Sybase, Teradata, Windows File Share, excluir IE, los hosts S-TAP de Windows también pueden utilizar los protocolos siguientes: MSSQL, conductos con nombre.

Ejemplo:

```
grdapi verify_stap_inspection_engine_with_sequence stapHost=9.70.144.212
sequence=3
```

revoke_ignore_stap

Este mandato revoca las acciones de reglas de política existentes IGNORE S-TAP SESSION (REVOKABLE) que omiten el tráfico de sesiones de S-TAP. Este mandato solo revoca las reglas de omisión flexibles (marcadas como REVOKABLE) y no puede revocar las reglas estrictas (no marcadas como REVOKABLE).

Tabla 8. revoke_ignore_stap

Parámetro	Descripción
stapHost	Necesario. El nombre de host o la dirección IP de un servidor de bases de datos en el que se han instalado y configurado los S-TAP para informar a este sistema Guardium, o una lista separada por comas de nombres de host o direcciones IP. También puede utilizar estos valores: all_active Todos los S-TAP configurados para informar a este sistema Guardium all_windows_active Todos los S-TAP configurados para informar a este sistema Guardium y que se ejecutan en máquinas Windows all_unix_active Todos los S-TAP configurados para informar a este sistema Guardium y que se ejecutan en máquinas UNIX
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo

```
grdapi revoke_ignore_stap stapHost=myhost1
```

set_ztap_logging_config

Este mandato controla los parámetros de registro que se describen a continuación.

Sintaxis: grdapi set_stap_logging_config parameter=[parameter] value=[value].

Tabla 9. Parámetros de set_ztap_logging_config

Parámetro	Valor	Descripción
log_db2z_target	0 para inhabilitar 1 para habilitar De forma predeterminada, el parámetro está inhabilitado.	Cuando se habilita utilizando `log_db2z_target=1`, se registran los destinos del mensaje db2z protobuf en GDM_OBJECT junto con los objetos del analizador.
log_zkey_to_full_sql	0 para inhabilitar 1 para habilitar De forma predeterminada, el parámetro está inhabilitado.	Cuando se habilita mediante `log_zkey_to_full_sql=1`, los valores de clave VSAM o IMS se registran en la sentencia SQL completa para políticas que utilizan "Detalles completos de registro".

Ejemplo

```
grdapi set_ztap_logging_config parameter=log_db2z_target value=1
```

Mostrar valores: grdapi get_ztap_logging_config.

Tema principal: Referencia de GuardAPI

Funciones de detección de amenazas de GuardAPI

enable_advanced_threat_scanning

Habilita procesos de escaneado para comprobar si hay ataques específicos en bases de datos, tales como la inyección de SQL y procedimientos almacenados maliciosos.

Tabla 1. Parámetros de enable_advanced_threat_scanning

Parámetro	Descripción

Parámetro	Descripción
all	Opcional. Solo en una configuración de gestión central, habilita todos los escaneados de detección de amenazas en todas las unidades gestionadas. Valores permitidos: `true`, `false`.
schedule_start	Opcional. Especifica la fecha y hora para iniciar la ejecución de los procesos. El formato aceptado es aaaa-mm-dd hh:mm:ss (reloj de 24 horas).
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

```
grdapi enable_advanced_threat_scanning all=true schedule_start="2016-03-24 12:00:05”
```

Verá el mensaje siguiente si se ha habilitado el análisis de amenazas, cuando la detección de valor atípico no es:

```
Aviso: Habilitando el escaneo de amenazas avanzado (también conocido como Ojo de águila) cuando la detección de anomalías
analíticas está inhabilitada.
El escaneo de amenazas avanzado (también conocido como Ojo de águila) se ha habilitado.
ok
```

disable_advanced_threat_scanning

Inhabilita el escaneado de detección de amenazas en el explorador.

Tabla 2. Parámetros de disable_advanced_threat_scanning

Parámetro	Descripción
all	Solo en una configuración de gestión central, inhabilita todos los escaneados de detección de amenazas en todas las unidades gestionadas.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

get_eagle_eye_info

Muestra los valores actuales de los parámetros de detección de amenazas.

Tabla 3. Parámetros de get_eagle_eye_info

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

```
grdapi get_eagle_eye_info
Eagle Eye Parameters Values:
EI_CASES_DISPLAY_LIMIT = 3
EI_CONFIDENCE_PCT_CHANGE_TO_REDISPLAY_CASE = 30
EI_EAGLE_EYE_ENABLED = 1
EI_PROCESSOR_TIMEOUT_SEC = 420
EI_SCANNER_PATCH_DEF = 10
EI_SCANNER_TIMEOUT_SEC = 300ok
```

set_eagle_eye_parameter

Utilícelo bajo la dirección del personal de IBM. Cambia los parámetros de configuración para la detección de amenazas. Estos parámetros se deben establecer de forma explícita utilizando `parameter_name` y `parameter_value` como se indica a continuación:

```
set_eagle_eye_scanner_parameter parameter_name=[parameter] parameter_value=[value]
```

Tabla 4. Parámetros de set_eagle_eye_parameter

Parámetro	Descripción
EI_CASES_DISPLAY LIMIT	El número de casos que se van a mostrar en el informe de la lista de tareas pendientes. El valor predeterminado es 3.
EI_CONFIDENCE_PCT_CHANGE _TO_REDISPLAY CASE	El porcentaje de cambio de "confianza" que provocará que este caso se vuelva a visualizar en el informe de lista de tareas pendientes, aunque ya se haya incluido antes. Esto puede suceder si Guardium detecta otro síntoma o síntomas que aumentan la confianza con este valor de porcentaje. El valor predeterminado es 30.
EI_PROCESSOR_TIMEOUT_SEC	Los procesadores que se ejecutan durante más tiempo que el valor de este umbral se desactivan. El valor predeterminado es de 420 segundos.
EI_SCANNER_PATCH_DEF	Para evitar falsos positivos como resultado de la instalación de parches, si en una sola ejecución del proceso el número de procedimientos almacenados creados supera este parámetro, el proceso presupone que se ha instalado un parche y detiene el análisis de los síntomas. El valor predeterminado es de 10 creaciones de procedimientos almacenados detectadas en una sola ejecución.
EI_SCANNER_TIMEOUT_SEC	Los procesos de escaneado que se ejecutan durante más tiempo que el valor de este umbral se desactivan. El valor predeterminado es de 300 segundos.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

get_eagle_eye_scanners_info

Devolver información acerca de los valores de escaneado.

Tabla 5. Parámetros de get_eagle_eye_scanners_info

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Los datos devueltos contienen la información siguiente:

Tabla 6. Parámetros de get_eagle_eye_scanners_info

Campo	Descripción
ID	El ID del escáner.
Name	El nombre del escáner.
Status	Estado del escáner de la última ejecución: I: En curso D: Hecho K: Interrumpido E: Hecho con errores
Enabled	Indica si está habilitado el escáner. True: Habilitado False: Inhabilitado

Campo	Descripción
Permanent disabled	Si se ha inhabilitado el escáner 3 veces en 24 horas, se inhabilita de forma permanente. True: Inhabilitado False: Habilitado

Ejemplo:

```
grdapi get_eagle_eye_scanners_info
ID=0
ID:1, Name:SQLInjectionExceptionsScanner, Status:D, Enabled:true, Permanent disabled:false
ID:2, Name:NumNewConstructScanner, Status:D, Enabled:true, Permanent disabled:false
ID:3, Name:SQLInjectionSuspiciousObjectScanner, Status:D, Enabled:true, Permanent disabled:false
ID:4, Name:SqliQueryScanner, Status:Unknown, Enabled:false, Permanent disabled:true
ID:5, Name:EagleEyeSTPCreateProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:6, Name:EagleEyeSTPCallProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:7, Name:EagleEyeSTPExceptionProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:8, Name:EagleEyePreviousStpUsageProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:9, Name:EagleEyeSTPViolationProcedureScanner, Status:D, Enabled:true, Permanent disabled:false
ID:10, Name:EagleEyeSTPUserOutlierScanner, Status:D, Enabled:true, Permanent disabled:false
ok
```

set_eagle_eye_scanner_parameter

Utilícelo bajo la dirección del personal de IBM. Activa o desactiva un escáner. Estos parámetros se deben establecer de forma explícita utilizando `parameter_name` y `parameter_value` como se indica a continuación:

```
set_eagle_eye_scanner_parameter parameter_name=[parameter] parameter_value=[value]
```

Tabla 7. Parámetros de set_eagle_eye_scanner_parameter

Parámetro	Descripción
scanner_id	Necesario. El ID exclusivo del escáner, que puede obtener con el mandato de GuardAPI get_eagle_eye_scanners_info.
is_active	Define si el escáner se debe ejecutar. Se utiliza para iniciar un escáner que se ha detenido automático porque ha excedido el tiempo de espera. 0: Se ha detenido el escáner 1: Se ha activado el escáner
is_permanent_inactive	Si se ha inhabilitado el escáner 3 veces en 24 horas, entonces solo se puede volver a habilitar utilizando este mandato de GuardAPI. 1: El escáner se ha detenido de forma permanente 0: El escáner está habilitado
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

El siguiente ejemplo vuelve a activar un escáner desactivado de forma permanente.

```
set_eagle_eye_scanner_parameter scanner_id=2 parameter_name=is_permanent_inactive parameter_value=0
```

get_eagle_eye_symptom_period_hours

Mostrar el valor del parámetro de periodo de sistema en horas. El periodo de síntoma determina durante cuánto tiempo el proceso está buscando y analizando los síntomas recopilados para un caso.

Tabla 8. Parámetros de get_eagle_eye_symptom_period_hours

Parámetro	Descripción
case_name	Necesario. El tipo de caso. Se permiten los valores siguientes: STP: Caso de procedimiento almacenado malicioso SQL_INJECTION: Caso de inyección de SQL

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

```
grdapi get_eagle_eye_symptom_period_hours case_name=STP
The symptoms period for case type: STP is: 168 in hours
ok
```

set_eagle_eye_symptom_period_hours

Establece un valor para el parámetro de periodo de sistema en horas. El periodo de síntoma determina durante cuánto tiempo el proceso está buscando y analizando los síntomas recopilados para un caso.

Tabla 9. Parámetros de set_eagle_eye_symptom_period_hours

Parámetro	Descripción
case_name	Necesario. El tipo de caso. Se permiten los valores siguientes: STP: Caso de procedimiento almacenado malicioso SQL_INJECTION: Caso de inyección de SQL
symptom_period_hours	Necesario. Entero. El número de horas anteriores para analizar los síntomas de un caso.
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

```
grdapi set_eagle_eye_symptom_period_hours case_name=STP symptom_period_hours=170
The symptoms period for case type: STP was changed. The old value was: 168. The new value is: 170
ok
```

get_eagle_eye_debug_level

Para uso del personal de IBM. Muestra el nivel de depuración actual:

- 1: Activado
- 0: Desactivado

Tabla 10. Parámetros de get_eagle_eye_debug_level

Parámetro	Descripción
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

```
grdapi get_eagle_eye_debug_level
ID=0
component=EAGLE_EYE level=1
ok
```

set_eagle_eye_debug_level

Para uso del personal de IBM. Muestra el nivel de depuración actual.

Tabla 11. Parámetros de set_eagle_eye_debug_level

Parámetro	Descripción
level	Entero. Necesario. Valores permitidos: 1: Activado 0: Desactivado
api_target_host	Parámetro opcional que especifica los hosts de destino para ejecutar la API.Cuando no se especifica, toma como valor predeterminado la unidad en la que se ejecuta el mandato. Valores válidos: • all_managed: para todas las unidades gestionadas • all: todas las unidades gestionadas y Gestor central (CM) • group: <nombre grupo>: donde el nombre de grupo es un grupo de unidades gestionadas • desde un CM únicamente, el nombre de host o la dirección IP de las unidades gestionadas, por ejemplo, `api_target_host=10.0.1.123` • desde una unidad gestionada, el nombre de host o la dirección IP del Gestor central (CM) Guardium V10.1 y 10.1.2: Únicamente en una configuración de gestión central, especifica un host de destino donde se ejecutará la API. En un Gestor central (CM), el valor es el nombre de host o la IP de cualquier unidad gestionada. En una unidad gestionada, es el nombre de host o la IP del CM.

Ejemplo:

```
grdapi set_eagle_eye_debug_level level=0
ID=0
ok
```

Tema principal: Referencia de GuardAPI

S-TAP for z/OS V10.1.3 User's Guide

- **IBM Security Guardium S-TAP for Db2 on z/OS**
  These topics describe how to use IBM® Security Guardium® S-TAP® for DB2® on z/OS® V10.1.3 (also referred to as IBM Guardium S-TAP for Db2). The V10.1.3 S-TAP is optimized for the V10.1 Guardium system. IBM Guardium S-TAP for Db2 collects and correlates data access information from a variety of Db2 resources to produce a comprehensive view of business activity for auditors.
- **IBM Security Guardium S-TAP for IMS on z/OS**
  These topics describe how to use IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 (also referred to as IBM Guardium S-TAP for IMS). The V10.1.3 S-TAP is optimized for the V10.1 Guardium system. IBM Guardium S-TAP for IMS collects and correlates data access information from a variety of IMS resources to produce a comprehensive view of business activity for auditors.
- **IBM Security Guardium S-TAP for Data Sets on z/OS**
  These topics describe how to use IBM Security Guardium S-TAP for Data Sets on z/OS V10.1.3 (also referred to as IBM Guardium S-TAP for Data Sets). The V10.1.3 S-TAP is optimized for the V10.1 Guardium system. IBM Guardium S-TAP for Data Sets collects and correlates data access information from a variety of resources to produce a comprehensive view of business activity for auditors.

IBM Security Guardium S-TAP for Db2 on z/OS

These topics describe how to use IBM Security Guardium S-TAP for Db2 on z/OS V10.1.3 (also referred to as IBM Guardium S-TAP for Db2). The V10.1.3 S-TAP is optimized for the V10.1 Guardium system. IBM Guardium S-TAP for Db2 collects and correlates data access information from a variety of Db2 resources to produce a comprehensive view of business activity for auditors.

About these topics

This information is designed to help database administrators, system programmers, and application programmers perform these tasks:

- Plan for the installation of IBM Guardium S-TAP for Db2
- Install and operate IBM Guardium S-TAP for Db2
- Configure the IBM Guardium S-TAP for Db2 environment
- Diagnose and recover from IBM Guardium S-TAP for Db2 problems

A PDF of this User's Guide is also available here.

- **IBM Security Guardium S-TAP for Db2 on z/OS overview**
  IBM Security Guardium S-TAP for Db2 on z/OS (also referred to as IBM Guardium S-TAP for Db2) collects and correlates data access information from Db2 to produce a comprehensive view of business activity for auditors. IBM Guardium S-TAP for Db2 enables you to determine which users updated or read a particular table, on a specific z/OS Db2 system, within a specific time period.
- **Configuring IBM Security Guardium S-TAP for Db2 on z/OS**
  After you install IBM Guardium S-TAP for Db2, you must customize some files for your system. All configuration steps are required in both stand-alone and data sharing environments.
- **Data collection**
  IBM Guardium S-TAP for Db2 collects data from an audited Db2 subsystem, in accordance with the collection policies that you create through the IBM Guardium system. Use a collection policy to specify filtering criteria that captures relevant data and filters out irrelevant data. The filtering criteria that you specify determines which data is streamed to your IBM Guardium system.
- **Reference information**
  These reference topics are designed to provide you with quick access to information about IBM Guardium S-TAP for Db2 sample library members, parameters, and variables.
- **Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS**

Parent topic: S-TAP for z/OS V10.1.3 User's Guide

IBM Security Guardium S-TAP for Db2 on z/OS overview

IBM Security Guardium S-TAP for Db2 on z/OS (also referred to as IBM Guardium S-TAP for Db2) collects and correlates data access information from Db2 to produce a comprehensive view of business activity for auditors. IBM Guardium S-TAP for Db2 enables you to determine which users updated or read a particular table, on a specific z/OS Db2 system, within a specific time period.

Use IBM Guardium S-TAP for Db2 to collect and correlate the following types of data to the Guardium system:

- Modifications to an object (SQL UPDATE, INSERT, DELETE)
- Reads of an object (SQL SELECT)
- Explicit GRANT and REVOKE operations to capture events where users might be attempting to modify authorization levels
- Assignment or modification of an authorization ID
- Authorization attempts that are denied because of inadequate authorization
- CREATE, ALTER, and DROP operations against an object (such as a table)
- Utility access to an object (IBM utilities only)
- Db2 commands entered, including which users are issuing specific commands

IBM Guardium S-TAP for Db2 uses Db2 data sharing to obtain audit information from all members of the data sharing group.

- **What's new in IBM Security Guardium S-TAP for Db2 on z/OS V10.1.3?**
  Version 10.1.3 of IBM Guardium S-TAP for Db2 provides speed and monitoring enhancements.
- **The IBM Security Guardium S-TAP for Db2 on z/OS installation environment**
  The IBM Guardium S-TAP for Db2 SQL Collector Agent collects data from an audited Db2 subsystem in accordance with the filtering policies you set with the Guardium system.
- **Installation and operation requirements**
  Verify that you have the hardware and software that is required to install and operate IBM Guardium S-TAP for Db2.

Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS

What's new in IBM Security Guardium S-TAP for Db2 on z/OS V10.1.3?

Version 10.1.3 of IBM Guardium S-TAP for Db2 provides speed and monitoring enhancements.

Enhancements to this version of the product include:

- New Simulation mode enables you to test policies without sending data to the appliance. Data is collected on z/OS.
- Support for the collection of BIND/REBIND events
- Support for the collection of CICS Unit of Work ID
- Improved memory management
- Support for blocking policies pushed-down from the appliance
- Improved filtering of events
- MODIFY command now collects more diagnostic information
- Ability to exclude host variables
- Support for initiating an appliance MUST GATHER command from z/OS
- Support for S-TAP logging
- Support for Internet Protocol version 6 (IPV6) introduced with PH16991

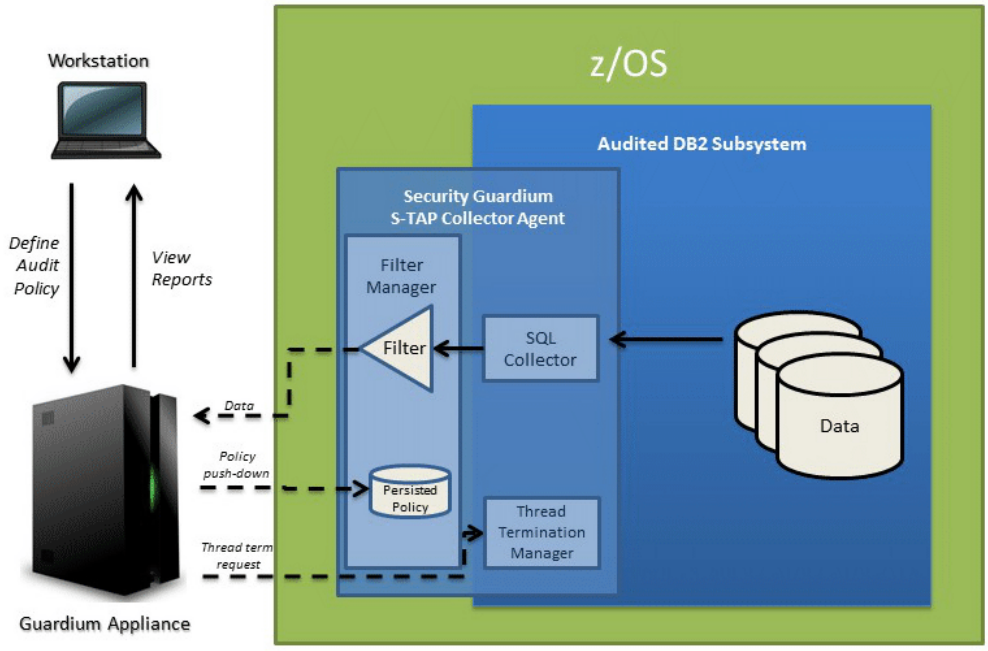
Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS overview

The IBM Security Guardium S-TAP for Db2 on z/OS installation environment

The IBM Guardium S-TAP for Db2 SQL Collector Agent collects data from an audited Db2 subsystem in accordance with the filtering policies you set with the Guardium system.

The IBM Guardium S-TAP for Db2 collector agent runs as a started task and is responsible for the collection of audit data in an IBM Guardium S-TAP for Db2 environment. As shown in the following diagram, SQL collector data is filtered and sent to the Guardium system, enabling you to view reports on your workstation.

Figure 1. An overview of the IBM Guardium S-TAP for Db2 environment



Guardium Appliance System

The Guardium system can gather, and report on, information from multiple agents running on multiple z/OS systems. The Guardium system:

- Provides the user interface, which processes requests and displays the resulting information.
- Enables you to create filtering policies, which specify the types of data to be collected by the agent.
- Stores the collected data.

Guardium Appliance System and S-TAP Collector Agent communication

The Guardium system and the IBM Guardium S-TAP for Db2 agent communicate by using a TCP/IP connection. The filtering policies that you create instruct the agent about the data to collect, such as which jobs and data sets to monitor for data accesses.

The IBM Guardium S-TAP for Db2 agent is responsible for:

- Collecting Db2 audit data based on the policy settings.
- Enabling activities to be blocked.
- Streaming collected event activity to the Guardium system.

For more information about how Guardium system policies are interpreted and enabled by the S-TAP, see Policy pushdown.

With the Guardium system installed, configured, and running in your environment, you can test your connection from the z/OS platform to the Guardium system by configuring and running the IBM Guardium S-TAP for Db2 sample library member, ADHTCPD. Consult your network security team to review the results and confirm that connection from the z/OS platform to the Guardium system is available.

Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS overview

Installation and operation requirements

Verify that you have the hardware and software that is required to install and operate IBM Guardium S-TAP for Db2.

FEC common code FMID H25F132 is required, and must be present on the system for the successful installation of this product.

IBM Db2 Data Access Common Collector for z/OS V1.1 (CQC) common code FMID HCQC110 is required, and must be present on the system for the successful installation of this product.

Hardware requirements

Any hardware that is capable of running Db2 for z/OS (V11 or later, until end of service).

Collector agent requirements

- Db2 Version 11 or later, until end of service.
- z/OS Version 2 Release 2 or later, until end of service.
- The IBM Guardium S-TAP for Db2 collector agent must be run on an operating system version that is equivalent to the operating system version on which the product SMP/E installation is performed.
- Resource Recovery Services (RRS) must be configured and enabled for IBM Guardium S-TAP for Db2 to use the RRSAF attachment facility to connect to Db2.

- **Compatibility with IBM Db2 Query Monitor for z/OS**
  IBM Guardium S-TAP for Db2 does not require Db2 Query Monitor to be installed or activated on a Db2 subsystem that IBM Guardium S-TAP for Db2 audits. If you are running Db2 Query Monitor on your system, be aware that IBM Guardium S-TAP for Db2 can audit a Db2 subsystem that is running Db2 Query Monitor Version 3.2 or later. Certain IBM Guardium S-TAP for Db2 PTFs require Db2 Query Monitor PTFs through SMP/E IFREQ.
- **Required user ID authorizations**
  To operate IBM Guardium S-TAP for Db2, the S-TAP collector agent started task must run under the authority of a Time Sharing Option (TSO) user ID with these authorizations.

Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS overview

Compatibility with IBM Db2 Query Monitor for z/OS

IBM Guardium S-TAP for Db2 does not require Db2 Query Monitor to be installed or activated on a Db2 subsystem that IBM Guardium S-TAP for Db2 audits. If you are running Db2 Query Monitor on your system, be aware that IBM Guardium S-TAP for Db2 can audit a Db2 subsystem that is running Db2 Query Monitor Version 3.2 or later. Certain IBM Guardium S-TAP for Db2 PTFs require Db2 Query Monitor PTFs through SMP/E IFREQ.

To implement Db2 Query Monitor, your site must have the appropriate operating system, environment, hardware, software, and network requirements. For information about installing and operating Db2 Query Monitor, refer to the IBM Db2 Query Monitor for z/OS Knowledge Center.

Compatible releases and maintenance levels

The following product abbreviations are used:

- InfoSphere® Guardium S-TAP for Db2: STP
- IBM Security Guardium S-TAP for Db2 on z/OS: STP
- Db2 Query Monitor: CQM

Table 1. Compatible releases and maintenance levels

	CQM 3.2	**CQM 3.3**	**STP 9.1**	**STP 10.0**	**STP V10.1.3**
CQM 3.2	---	LPAR	Db2	Db2	Db2
CQM 3.3	LPAR	---	Db2	Db2	Db2
STP 9.1	Db2	Db2	---	LPAR	LPAR
STP 10.0	Db2	Db2	LPAR	---	LPAR
STP 10.1.3	Db2	Db2	LPAR	LPAR	---

Where:

LPAR
: The two products releases can coexist on the same LPAR (provided they use a different MASTER name), but cannot be active on the same Db2 subsystem.

Db2
: The two products releases can coexist on the same LPAR and can both be active on the same Db2 subsystem/shared collector.

Parent topic: Installation and operation requirements

Required user ID authorizations

To operate IBM Guardium S-TAP for Db2, the S-TAP collector agent started task must run under the authority of a Time Sharing Option (TSO) user ID with these authorizations.

The collector agent user ID requires Db2 privileges. Grant the collector agent user ID SYSCTRL authority, and the authority to issue the SELECT statements on these tables:

- SYSIBM.SYSTABLES
- SYSIBM.SYSTABLESPACE
- SYSIBM.SYSINDEXES

OMVS segment

The collector agent uses UNIX System Services (USS) callable services as the network interface to the appliance. The USS callable services require that an OMVS segment is defined in the RACF® profile for the user ID under which the collector agent job runs. The OMVS segment that is defined for the user ID must contain the following minimum requirements:

- A numeric user ID that is assigned to the user
- A valid path to an existing home directory
- A program name, for example: /bin/sh or /bin/echo for non-shell
- A numeric group ID that is assigned to the user's DEFAULT group

To verify that the ID has an OMVS segment in its RACF profile, use the following command:

```
LU user ID OMVS
```

To add an OMVS segment to the RACF profile of an ID, refer to this sample command:

```
ALTUSER user ID
OMVS(UID(nnn)HOME('/u/ user ID)
PROGRAM('/bin/sh')
```

Parent topic: Installation and operation requirements

Configuring IBM Security Guardium S-TAP for Db2 on z/OS

After you install IBM Guardium S-TAP for Db2, you must customize some files for your system. All configuration steps are required in both stand-alone and data sharing environments.

Before you begin

Review the collector agent security and system requirements before proceeding with the following steps. A list of sample library members is provided in this User's Guide.

About this task

The following table describes the configuration steps and the corresponding SADHSAMP sample library member that is required for customization.

Table 1. Configuration steps

Step	Description of configuration step	SADHSAMP sample library member to use
1	APF authorizing the LOAD library data set	(Not applicable)
2	Customizing JCL members using the ADHEMAC1 macro	ADHEMAC1
3	Binding DBRMs using the JCL bind job	ADHBIND
4	Granting required authorizations to USERID and ADHPLAN by using the JCL authorization member	ADHGRANT
5	Creating the IBM Guardium S-TAP for Db2 control file	ADHSJ000
6	Configuring the IBM Guardium S-TAP for Db2 control file	ADHSJ001
7	Configuring the collector agent	ADHCFGP and ADHCSSID
8	Authorizing ADHPLCY for policy pushdown	Define ADHPLCY to RACF or an equivalent security system

- **Upgrading from IBM Guardium S-TAP for Db2 V9.0, V9.1, or V10.0**
  You can upgrade to IBM Guardium S-TAP for Db2 V10.1.3 from IBM Guardium S-TAP for Db2 V9.0, V9.1, or V10.0 by completing these steps.
- **Configuring IBM Security Guardium S-TAP for Db2 on z/OS**
  After installation, configure IBM Guardium S-TAP for Db2 by completing the steps that are described in this section.

Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS

Upgrading from IBM Guardium S-TAP for Db2 V9.0, V9.1, or V10.0

You can upgrade to IBM Guardium S-TAP for Db2 V10.1.3 from IBM Guardium S-TAP for Db2 V9.0, V9.1, or V10.0 by completing these steps.

Procedure

1. Complete the SMP/E installation of IBM Guardium S-TAP for Db2 V10.1.3.
2. APF-authorize the V10.1.3 SADHLOAD data set.
3. Customize and run the Db2 bind job in SADHSAMP(ADHBIND).
4. Customize and run the Db2 grant job in SADHSAMP(ADHGRANT).
5. Export and save your collection profiles.
   (V8.1 collection profiles, or policies, were administered either with the InfoSphere® Guardium S-TAP for Db2 administration client, or the IBM Guardium system.)
6. Stop the previous version's collector agent and server address spaces.
7. Update the collector started task JCLs (ADHC*ssid*) to:
   - Remove the previous version of the product SADHLOAD data sets.
   - Include the new V10.1.3 product SADHLOAD data sets in the STEPLIB DD concatenation members.

   Note: ADHS*ssid* and ADHA*ssid* started tasks are not used in IBM Guardium S-TAP for Db2 V10.1.3.
8. Update the V10.1.3 collector configuration member (typically SADHSAMP(ADHCFGP).
9. Install a collection policy on the IBM Guardium system.
   - If policy pushdown was used for V8.1 collection administration, follow the Guardium Policy Builder instructions for migrating policies for V8.1 to V10.1.3.
   - If the InfoSphere Guardium S-TAP for Db2 administration client was used for V8.1 collection administration, use the XML exported in Step 4 as a reference for the Guardium Policy Builder to define collection policies for V10.1.3.
10. Start the collector address space by typing `/S ADHC`*ssid* at the z/OS® command prompt.

What to do next

Now you can install policies on the z/OS host by using the IBM Guardium system interface. No additional configuration steps are required.
Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Configuring IBM Security Guardium S-TAP for Db2 on z/OS®

After installation, configure IBM Guardium S-TAP for Db2 by completing the steps that are described in this section.

- **APF authorizing the LOAD library data set**
  The system programmer must APF authorize the product LOAD library for data collection to work correctly. The system programmer must modify the IEAAPFxx or PROGxx PARMLIB members to define the IBM Guardium S-TAP for Db2 data set, as specified by ADHEMAC1 macro value #SADHLOAD, as an APF authorized library.

- **Enabling the dynamic LPA facility service CSVDYLPA**
  The user ID that was used to start the Collector Agent PROC must be enabled to use the dynamic LPA facility CSVDYLPA to enable the collector agent to collect data.
- **Service class considerations**
  The collector agent started task must be set at a dispatching priority that is the same as, or higher than, that of Db2.
- **Customizing JCL members**
  Use the edit macro ADHEMAC1 to customize the variables in the JCL to be run. Running ADHEMAC1 allows you to modify members without requiring you to remember plan names, creators, and other variables from one editing session to the next editing session.
- **Creating the IBM Guardium S-TAP for Db2 control file**
  IBM Guardium S-TAP for Db2 configuration information is stored in a VSAM data set, which is the product control file.
- **Configuring the IBM Guardium S-TAP for Db2 control file**
  IBM Guardium S-TAP for Db2 requires information that identifies target Db2 subsystems, product options, and data set attributes. The product configuration is saved in the VSAM product control file data set that you created previously.
- **Configuring the collector agent**
  To configure the collector agent, complete the steps provided in each of the subsequent sections. The address space dispatching priority for IBM Guardium S-TAP for Db2 must be the same as, or higher than, that of Db2.
- **Configuring the collector agent for additional Db2 subsystems**
  The collector agent must be configured for each Db2 subsystem that is to be audited.
- **Support Services Address Space overview**
  IBM Guardium S-TAP for Db2 uses a Support Services Address Space, also referred to as a Master Address Space. Learn about how the Master Address Space works, as well as the implications for using and stopping it.
- **Enabling CICS Login User ID reporting**
  You can capture the CICS® Login User ID for SQL Statements that are run in Db2 for CICS. The capture of CICS transactions is limited to CICS versions TS 4.2 or later, until end of support.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

APF authorizing the LOAD library data set

The system programmer must APF authorize the product LOAD library for data collection to work correctly. The system programmer must modify the IEAAPFxx or PROGxx PARMLIB members to define the IBM Guardium S-TAP for Db2 data set, as specified by ADHEMAC1 macro value #SADHLOAD, as an APF authorized library.

About this task

The IBM Guardium S-TAP for Db2 agent requires that all data sets accessed in the STEPLIB of the collector job be APF authorized, including:

- the LOAD library data set
- adhhlq.SADHLOAD
- the FEC data set fechlq.SFECLOAD (where *adhhlq* and *fechlq* are the data set high level qualifier where S-TAP and FEC products are installed)
- the CQC data set cqchlq.SCQCLOAD (where adhhlq and cqchlq are the data set high level qualifier where S-TAP and CQC products are installed)

Other data sets that require APF authorization are:

- CEE.SCEERUN
- CEE.SCEERUN2
- Db2 EXIT data set (i.e. DSN.VAR1.SDNEXIT)
- Db2 LOAD library data set (i.e. DSN.VAR1.SDSNLOAD)
- SYS1.LINKLIB

Refer to the *z/OS® Knowledge Center* for more information about how to APF authorize libraries.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Enabling the dynamic LPA facility service CSVDYLPA

The user ID that was used to start the Collector Agent PROC must be enabled to use the dynamic LPA facility CSVDYLPA to enable the collector agent to collect data.

About this task

Determine whether the dynamic LPA facility CSVDYLPA is SAF protected. If the dynamic LPA facility CSVDYLPA is not SAF protected, this step is not required.

Procedure

Provide the user ID with ADD/UPDATE/DELETE authority.
For more information about how to enable the CSVDYLPA resource, see section 5.6.3 of the *z/OS® V1R7.0 MVS™ Planning: Operations Guide* (SA22-7601-06), section *Controlling/Adding A Module to LPA after IPL*.
Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Service class considerations

The collector agent started task must be set at a dispatching priority that is the same as, or higher than, that of Db2.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Related tasks

- Configuring the collector agent

Customizing JCL members

Use the edit macro ADHEMAC1 to customize the variables in the JCL to be run. Running ADHEMAC1 allows you to modify members without requiring you to remember plan names, creators, and other variables from one editing session to the next editing session.

Procedure

1. Copy member ADHEMAC1 from the adhhilvl.SADHSAMP to your site's CLIST library, and then edit the ADHEMAC1 macro with the appropriate variables.
2. After you copy the edit macro to your CLIST library, use it to edit each sample library member individually. You might need to update the macro between edits depending on the member being edited and the context of the variable to be modified in the sample library.
3. To run the macro, type the ADHEMAC1 command to automatically update the appropriate variables in the member that you are editing.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Related reference

- ADHEMAC1 edit macro variables

Creating the IBM Guardium S-TAP for Db2 control file

IBM Guardium S-TAP for Db2 configuration information is stored in a VSAM data set, which is the product control file.

About this task

Using the sample JCL that is included with the product, complete these steps to create the IBM Guardium S-TAP for Db2 control file:

Procedure

1. Edit SADHSAMP member ADHSJ000.
2. Add the appropriate job card to ADHSJ000.
3. In the DELETE instruction, change the data set name.
4. In the DEFINE CLUSTER instruction, change the following text within parentheses:
   - Data set NAME
   - VOLUMES
   - DATA NAME
   - INDEX NAME
5. In the REPRO instruction, change the name of the OUTDATASET.
6. Run ADHSJ000 to create the control file. The job steps must end with a return code of zero.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Configuring the IBM Guardium S-TAP for Db2 control file

IBM Guardium S-TAP for Db2 requires information that identifies target Db2 subsystems, product options, and data set attributes. The product configuration is saved in the VSAM product control file data set that you created previously.

About this task

Update the product control file by using the sample JCL that is included with IBM Guardium S-TAP for Db2. Sample library member ADHSJ001 contains the JCL to update the control file. The following steps list the tasks required to configure the product control file data set.
Important: The Db2 plan names that are specified in the product configuration options must match the product plan names assigned to the product's Db2 plans bind plan job.

Procedure

1. Edit SADHSAMP member ADHSJ001.
2. Add the appropriate job card to ADHSJ001.
3. Change ADH.V0A00.CONTROL to the name of the VSAM control data set that you created using member ADHSJ000.
4. Change #SADHLOAD to the name of the product LOADLIB used for IBM Guardium S-TAP for Db2.
5. Modify the SYSIN DD statements as instructed in the sample member. For more information, see Required statements for each subsystem.
   Important: In a data-sharing environment, specify subsystem names (not group names) in ADHSJ001.
6. Run ADHSJ001.
   Ensure that the update job steps of the product control file end with a return code of zero. If a non-zero return code occurs, review the job output for errors, correct the problem, and resubmit the JCL.

- **Required statements for each subsystem**
  The following statements are required for each Db2 subsystem that is added to the control file.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Required statements for each subsystem

The following statements are required for each Db2 subsystem that is added to the control file.

Table 1. Required statements for

each subsystem

Statement	Setting
SET DB2 SSID	#SSID
UPDATE DB2 ZPARMS	#SZPARM
UPDATE DB2 BOOTSTRAP 1	#SBSDS01
UPDATE DB2 LOADLIB 1	#SDSNEXIT
UPDATE DB2 LOADLIB 2	#SDSNLOAD
SET PRODUCT CFG	NULL
SET PRODUCT VER	NULL
UPDATE ADH PLAN 1	ADHPLAN1
UPDATE ADH CORR ID 1	ADH ID 1
UPDATE ADH CORR ID 2	ADH ID 2

Parent topic: Configuring the IBM Guardium S-TAP for Db2 control file

Configuring the collector agent

To configure the collector agent, complete the steps provided in each of the subsequent sections. The address space dispatching priority for IBM Guardium S-TAP for Db2 must be the same as, or higher than, that of Db2.

1. Configuring the JCL for ADHBIND
   SADHSAMP(ADHBIND) is a job that binds the packages and plan used by the collector agent.
2. Configuring the JCL for ADHGRANT
   SADHSAMP(ADHGRANT) is a job that grants authorizations to the user ID and plan that are used by the collector agent.
3. Configuring the ADHCFGP data set
   The ADH#MAIN program uses parameters to define the IBM Guardium S-TAP for Db2 subsystem name, the monitored Db2 subsystem, the Guardium system host name or network address TCP/IP port, and other parameters that control how the IBM Guardium S-TAP for Db2 collector agent is implemented.
4. Defining the collector agent started task JCL
   The collector agent runs as a started task. The sample library member ADHC*SSID* contains the sample JCL to set up the IBM Guardium S-TAP for Db2 collector agent started task.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Related reference

- Service class considerations

Configuring the JCL for ADHBIND

SADHSAMP(ADHBIND) is a job that binds the packages and plan used by the collector agent.

Procedure

1. Customize and submit the JCL according to the instructions in the member.
2. Submit the ADHBIND JCL to bind the collector agent packages and plan on each Db2 subsystem on which you want to use IBM Guardium S-TAP for Db2.

Parent topic: Configuring the collector agent
Next topic: Configuring the JCL for ADHGRANT

Configuring the JCL for ADHGRANT

SADHSAMP(ADHGRANT) is a job that grants authorizations to the user ID and plan that are used by the collector agent.

Procedure

1. Customize and submit the JCL according to the instructions in the member.
2. Submit the ADHGRANT JCL to grant authorizations to the user ID and plan that are used by the collector agent for each Db2 subsystem on which you want to use IBM Guardium S-TAP for Db2.
   Note: The ADHGRANT job contains examples of the GRANTs that meet the minimal authorization requirements for the collector agent. Alternative authorizations and, subsequently, GRANTs, can be used to meet the minimal authorization requirements for the collector agent.

Parent topic: Configuring the collector agent
Previous topic: Configuring the JCL for ADHBIND
Next topic: Configuring the ADHCFGP data set

Configuring the ADHCFGP data set

The ADH#MAIN program uses parameters to define the IBM® Guardium® S-TAP® for DB2® subsystem name, the monitored Db2 subsystem, the Guardium system host name or network address TCP/IP port, and other parameters that control how the IBM Guardium S-TAP for Db2 collector agent is implemented.

About this task

These parameters are defined in an 80-byte sequential or partitioned data set that you must allocate to the ADHPARMS DD. A sample is available in the SADHSAMP library member ADHCFGP.

Note: The AUDIT parameter is required. It instructs the collector agent to audit a specific Db2 subsystem. It supports only one Db2 subsystem.

To use the sample ADHCFGP member:

Procedure

1. Copy ADHCFGP to the appropriate location (PARMLIB) on your system.
2. Verify that the parameters are valid for your environment. If necessary, edit the parameter file for your IBM Guardium S-TAP for Db2 objects.
3. Edit the ADHPARMS DD in the started task JCL to point to the ADHCFGP data set that you have customized.

Example

An example of the ADHCFGP member contents is as follows:

```
BROWSE    ADH.SMPE.SAMPLIB(ADHCFGP) - 01 L
Command ===>
SUBSYS(#SSID)
AUDIT(#SSID)
MASTER_PROCNAME(ADHMST31)
APPLIANCE_SERVER(#APPSRVR)
```

Parent topic: Configuring the collector agent
Previous topic: Configuring the JCL for ADHGRANT
Next topic: Defining the collector agent started task JCL

Defining the collector agent started task JCL

The collector agent runs as a started task. The sample library member ADHC*SSID* contains the sample JCL to set up the IBM Guardium S-TAP for Db2 collector agent started task.

Before you begin

To run the collector agent as a started task, the JCL must be in a cataloged procedure library. Modify the sample started task JCL in SADHSAMP library member ADHC*SSID* for your site, according to the instructions in the member.

About this task

The started task requires:

- READ access to the ADHCFGP data set in the RACF® DATASET class
- UPDATE access to the DB2PARMS data set in the RACF DATASET class
- The ability to connect to the Db2 subsystem that is monitored by the collector agent
- The ability to read data from the following Db2 subsystem catalog tables:
  - SYSTABLES
  - SYSINDEXES
  - SYSDBRM
  - SYSPACKAGE
  - SYSPACKSTMT
  - SYSSTMT

Procedure

1. Using the sample library member ADHC*SSID* as a template, customize the member according to the directions contained in the sample JCL. Any valid member name can be used for the started task name, but the suggested started task name is ADHC*SSID*, where *SSID* is the identifier of the Db2 subsystem that is to be monitored.
2. Copy the customized JCL to an appropriate SYSPROC data set. The JCL must include definitions for the following data descriptions:

   ADHPARMS
   : ADHPARMS must name the IBM Guardium S-TAP for Db2 collector agent configuration file.

   DB2PARMS
   : DB2PARMS must name the IBM Guardium S-TAP for Db2 product control file (example: ADH.V0A00.CONTROL).

   ADHPLCY
   : ADHPLCY enables policy persistence. For more information, see the Policy Persistence information provided in Policy pushdown.
   If ADHPLCY is defined, it must point to a data set that is allocated with a record format of fixed blocked (RECFM=FB) and a record length (LRECL) greater than or equal to 256.
   The ADHPLCY data set should be allocated with a minimum of 50 primary tracks and 10 secondary tracks. The ADHPLCY data set can be sequential, PDS, or PDS/E. If you use PDS or PDS/E, the space requirements might need to be increased in relation to the number of members that are contained within the data set.

   ADHLOG
   : ADHLOG is the SYSOUT data set to which IBM Guardium S-TAP for Db2 collector agent log messages will be written.

   STEPLIB
   : STEPLIB must include the IBM Guardium S-TAP for Db2 SADHLOAD data set.
   Note: Every data set allocated to STEPLIB must be APF-authorized.

   SYSPRINT
   : SYSPRINT is the SYSOUT data set to which log messages will be written.

Parent topic: Configuring the collector agent
Previous topic: Configuring the ADHCFGP data set

Related reference

- Sample library members

Configuring the collector agent for additional Db2 subsystems

The collector agent must be configured for each Db2 subsystem that is to be audited.

Before you begin

You must have the following user ID authorities:

- READ access to ADHCFGx parameter data sets, Db2 catalogs, and VSAM control data sets
- Access to the DSNR resource class in Db2
- OMVS segment definition
- GRANT authority for SYSCTRL Db2 to communicate with the agent started task user IDs on all Db2 subsystems to be audited
- READ authority for the Db2 catalog tables
- Authority to use the dynamic LPA facility CSVDYLPA

To define additional Db2 subsystems for auditing, follow these steps:

Procedure

1. For additional stand-alone Db2 subsystems, use the SADHSAMP member ADHBIND to bind IBM Guardium S-TAP for Db2 plans on each Db2 subsystem that is to be audited.
   - For data sharing group members, use ADHBIND to bind one member of the data sharing group. The bind will apply to all additional group members.
   - When configuring the product control file for each member of the data sharing group, the PLAN value that is used in the ADHBIND job can also be used for the ADHPLAN1 value in the SJ001 JCL job.
   - For the first member of the data sharing group, PACKAGES and PLANS that are used in the ADHBIND job will work for all members of the data sharing group.
2. For each data sharing group or additional stand-alone Db2 subsystem, grant EXECUTE permission for the agent started task ID to the ADH PLAN 1, as specified in the PCF file for the Db2 subsystem. Refer to the JCL SADHSAMP member ADHGRANT for additional details on granting EXECUTE permission to the ADH PLAN.
3. Update the control file with the new SSID, or create a new S-TAP control file for each SSID by using the SADHSAMP member ADHSJ001.
4. Configure a new S-TAP agent configuration file.
5. Add the agent started task name to the z/OS® started task table.
6. Start the new S-TAP agent.
   Note:
   - Dispatching priority must be the same as, or higher than, Db2.

   After you start the agent, review the agent log and MVS™ log for any error messages. When an active collection policy is received, the agent starts collecting audit data.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Support Services Address Space overview

IBM Guardium S-TAP for Db2 uses a Support Services Address Space, also referred to as a Master Address Space. Learn about how the Master Address Space works, as well as the implications for using and stopping it.

A Support Services Address Space, also referred to as a Master Address Space, starts for each z/OS® image after the first instance of IBM Guardium S-TAP for Db2, InfoSphere® Optim™ Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS starts with a MASTER_PROCNAME value that is not yet in use on that z/OS image.

The Master Address Space is a Service Address Space for all instances of IBM Guardium S-TAP for Db2, InfoSphere Optim Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS that specify the same MASTER_PROCNAME parameter value that is running on the z/OS image. The Master Address Space acts as a placeholder for shared collector resources, and is similar to other Master Address Spaces that are used throughout MVS™. For sample, MVS and Db2 both have Master Address Spaces.

The Master Address Space:

- Never shuts down
- Does not run any code except for its initialization routines
- Owns resources that are needed by the shared collector
- Does not require a formal shutdown and should not be canceled or forced to shut down during the operation of IBM Guardium S-TAP for Db2, InfoSphere Optim Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS.
- Forcing the Master Address Space to stop causes the abnormal termination of all IBM Guardium S-TAP for Db2, InfoSphere Optim Query Workload Replay for Db2, and IBM Db2 Query Monitor for z/OS subsystems on the LPAR.

Important: During installation, do not stop or start the Master Address Space unless required by product maintenance or instructed to do so by IBM Software Support.

- **Usage considerations for the Master Address Space**
  The following considerations apply to the use of the Support Services Address Space when you are using IBM Guardium S-TAP for Db2 to monitor the same Db2 subsystem, or multiple Db2 subsystems, on the same LPAR.
- **Stopping the Master Address Space**
  Do not stop the Master Address Space unless you are directed to do so by IBM Software Support or by a ++HOLD(ACTION) in a PTF.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Usage considerations for the Master Address Space

The following considerations apply to the use of the Support Services Address Space when you are using IBM Guardium S-TAP for Db2 to monitor the same Db2 subsystem, or multiple Db2 subsystems, on the same LPAR.

Monitoring the same Db2 subsystem

If you use multiple collector products (such as IBM Guardium S-TAP for Db2, InfoSphere® Optim™ Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS®) to monitor the same Db2 subsystem, each product must specify the same value for the MASTER_PROCNAME parameter.

Monitoring multiple Db2 subsystems that reside on the same LPAR

If you use multiple collector products (such as IBM Guardium S-TAP for Db2, InfoSphere Optim Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS) or multiple instances of the same product to monitor different Db2 subsystems that reside on the same LPAR, each product can have a different value for the MASTER_PROCNAME parameter.

Note: This rule applies to instances when you are running different maintenance levels of the same product on the same LPAR (for example, if you are testing new maintenance levels prior to upgrading your production system).

Parent topic: Support Services Address Space overview

Stopping the Master Address Space

Do not stop the Master Address Space unless you are directed to do so by IBM Software Support or by a ++HOLD(ACTION) in a PTF.

To ensure product stability, the Master Address Space should only be stopped by using the sample job that is provided in SADHSAMP, member ADHMSTR. This job verifies that no IBM Guardium S-TAP for Db2, InfoSphere® Optim™ Query Workload Replay for Db2, or IBM Db2 Query Monitor for z/OS® subsystems are using the Master Address Space before it is stopped.

Parent topic: Support Services Address Space overview

Enabling CICS Login User ID reporting

You can capture the CICS® Login User ID for SQL Statements that are run in Db2 for CICS. The capture of CICS transactions is limited to CICS versions TS 4.2 or later, until end of support.

About this task

Update the CICS Connection definition to capture the CICS Login User ID:

Procedure

1. Set the ATTACHSEC parameter to ATTACHSEC(IDENTIFY) for the user ID to be passed from the Terminal-Owning Region (TOR) to the Application-Owning Region (AOR).
   This makes the user ID available for collection.
2. Ensure that the CICS_USERID collector agent parameter is set to *Y* to enable reporting of the CICS login user ID. For more information, see Collector agent parameters.

Results

The CICS Login User ID is reported in Guardium interface DB2 Client Info field for SQL Statements that are run in Db2 for CICS transactions.

Parent topic: Configuring IBM Security Guardium S-TAP for Db2 on z/OS

Data collection

IBM Guardium S-TAP for Db2 collects data from an audited Db2 subsystem, in accordance with the collection policies that you create through the IBM Guardium system. Use a collection policy to specify filtering criteria that captures relevant data and filters out irrelevant data. The filtering criteria that you specify determines which data is streamed to your IBM Guardium system.

You can define and manage data collection and filtering in the Guardium Policy Builder of the IBM Guardium system interface.

- **Data collection process**
  During the collection process, IBM Guardium S-TAP for Db2 collects event data and verifies the data against the collection criteria that is defined in the collection policy.
- **Filtering**
  IBM Guardium S-TAP for Db2 V10.1.3 greatly simplifies the filtering process from that which was used in past product versions. All filtering occurs at the point of collection regardless of the field types that are included in the rules for the active collection policy. Filtering occurs at the point of collection with or without the specification of object types, which results in efficient CPU usage.
- **Policy pushdown**
  At startup, the IBM Guardium S-TAP for Db2 collector agent waits for a policy to be streamed (or pushed down) from the Guardium system before activating a collection. When the collector agent receives a policy, it inactivates the active collection (if a collection is active), updates the collection profile with the new policy, and then activates the collection policy.
- **Streaming audit data to multiple systems**
  Multistream mode enables S-TAP audit events to be sent to multiple connected appliances. You can enable multistreaming to up to 6 Guardium appliances (APPLIANCE_SERVER + APPLIANCE_SERVER_*n*, where *n* can be 1 - 5).
- **Starting and stopping the collector agent**
  After you configure the product and review the data collection information, you can start the collector agent. Use the commands provided to start and stop the collector agent started task from a cataloged procedure library.
- **Including or excluding failed accesses and negative SQL code**
  IBM Guardium S-TAP for Db2 enables you to include or exclude failed accesses and negative SQL code on a per-policy basis.
- **Quarantining SQL activity**
  IBM Guardium S-TAP for Db2 enables you to quarantine the SQL activity of specific users for specific periods of time.
- **SQL Blocking**
  You can block the SQL activity of Db2 users' (Auth IDs) access to specific tables and databases. SQL statements that are run against accelerated tables are eligible for blocking if the blocking filtering criteria is met. If a SQL statement matches the blocking criteria, the SQL statement is prevented from running. Use the Guardium appliance interface to define blocking policies.

- **Controlling host variable collection**
  IBM Guardium S-TAP for Db2 enables you to specify, on a per-rule basis, whether host variable information will be sent to the appliance for activity that matches that rule.
- **Collecting Command activity by using the Audit SQL Collector**
  IBM Guardium S-TAP for Db2 enables you to collect Command activity by using the Audit SQL Collector.
- **Collecting SET CURRENT SQLID events by using the Audit SQL Collector**
  IBM Guardium S-TAP for Db2 V10.1.3 enables you to collect SET CURRENT SQLID events by using the Audit SQL Collector.

Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS

Data collection process

During the collection process, IBM Guardium S-TAP for Db2 collects event data and verifies the data against the collection criteria that is defined in the collection policy.

Collection includes the following:

- All reads and all changes (with collector agent based collection)
- Host variables up to a maximum of 256 bytes per variable
- Dynamic SQL text up to 2 million bytes per statement
- Static SQL text up to 4000 bytes

Data collected from Db2 is filtered during the collection process, and non-relevant events are discarded. Specify filtering criteria by defining a collection policy so that only relevant events are captured. This limits the amount of unnecessary data that is collected and stored by IBM Guardium S-TAP for Db2.

- **Collection policy**
  The collection policy is defined by the Guardium policy. It is used to determine which events (SQL, Command, Utilities, etc.) are streamed from the z/OS collector agent to the Guardium appliance. The following methodology determines how the collection policy determines whether to stream events to the Guardium appliance.
- **Collected event types**
  All event types are collected with the SQL Collection mechanism, which is not dependent on other SQL Trace information such as the Db2 Trace (IFI) or SMF data. Filtering criteria is defined and managed through the IBM Guardium system interface. This table lists the types of events that can be collected.

Parent topic: Data collection

Collection policy

The collection policy is defined by the Guardium policy. It is used to determine which events (SQL, Command, Utilities, etc.) are streamed from the z/OS collector agent to the Guardium appliance. The following methodology determines how the collection policy determines whether to stream events to the Guardium appliance.

The collection policy is comprised of one or more rules. Each rule includes a list of filtering criteria (fields), which is used to determine the events that are streamed. An event is streamed to the appliance if the fields within the event match all of the fields defined within any rules of the collection policy. (Evaluation of the rules within the collection policy is *or*.) For example, if a collection policy is composed of three rules (rule 1, rule 2, and rule 3), an event is streamed if it matches rule 1, or rule 2, or rule 3.

Each rule is made up of filter types and values (fields) that are used to determine if an event should be collected. If the fields of the rule are equivalent to the corresponding fields in the event, the rule evaluates the event to be true, or a match, and the event is captured. A rule is considered true if one of each specified filter type and value matches that of the event. (Evaluation of the rule is *and*.) For example:

- If a rule is comprised of the filters DBUser=`User1` and PLAN=`DSNTEP2`, an event is collected by the rule if both DBUser=`User1` and PLAN=`DSNTEP2` are present in the event. If only one of the filtering criterion is present, or neither of the filtering criteria are present, the event does not meet the conditions of the rule and will not be collected by the rule.
- If a rule is comprised of the filters NET_PROTOCOL=`TSO` and OS_USER=`User1`, then only TSO workload events executed by User1 will be collected by the rule (wherein User1 is Original Auth ID). Non-TSO workloads run by User1 will not be collected by the rule, nor will TSO workloads run by User2.

The following sections further describe how to filter the collector agent.

Parent topic: Data collection process

Collected event types

All event types are collected with the SQL Collection mechanism, which is not dependent on other SQL Trace information such as the DB2® Trace (IFI) or SMF data. Filtering criteria is defined and managed through the IBM® Guardium® system interface. This table lists the types of events that can be collected.

Table 1. Collected event types

Collected event types
All reads (SQL SELECT)
All changes (SQL UPDATE, INSERT, DELETE)
Authorization
Audit data for Db2 utilities
Grant/Revoke
Access attempts
Binds/Rebinds
Commit/Rollbacks
Db2 commands
Db2 utilities
Failed logins
Create, Alter, Drop table
Create, Alter, Drop all other object types

Collected event types
Static SQL host variables
Static SQL text
Dynamic SQL host variables
Dynamic SQL text
Negative SQL events
SQL events involving Accelerated/IDAA tables

Information collected for CICS events

For events that are collected with Net Prtcl of a type that originates from CICS, the Internet Protocol (IP) address is reported as Terminal ID and the CICS End User is reported as the DB2 User Name in the IBM Guardium system interface.

- **Audit data for Db2 Utilities**
  You can collect table information for Db2 utility operations that are run against tablespaces. The IBM Guardium S-TAP for Db2 collector agent reports the name of the table associated with the tablespace. Configure audit data for Db2 utilities according to the following rules.

Parent topic: Data collection process

Audit data for Db2 Utilities

You can collect table information for Db2 utility operations that are run against tablespaces. The IBM Guardium S-TAP for Db2 collector agent reports the name of the table associated with the tablespace. Configure audit data for Db2 utilities according to the following rules.

Set the STAP_UTILITY_TS_TO_TABLE parameter to `Y` to collect audit data for Db2 utilities. See Collector agent parameters for more information.
Audit data for Db2 utilities is collected according to the following rules:

- When a single table is contained in the tablespace, the table information is reported.
- When more than one table is contained in the tablespace, the product can be configured to report either:

  No tables
  : The tablespace is reported, but no tables are reported.

  All tables in the tablespace
  : Utility operations are reported against the accessed table.
  This option can result in false positives being reported against tables in the tablespace that were not affected by the running of the utility.

Parent topic: Collected event types

Filtering

IBM Guardium S-TAP for Db2 V10.1.3 greatly simplifies the filtering process from that which was used in past product versions. All filtering occurs at the point of collection regardless of the field types that are included in the rules for the active collection policy. Filtering occurs at the point of collection with or without the specification of object types, which results in efficient CPU usage.

Filtering occurs when you create a filter that uses one or more of the following filter fields:

Net Prtcl
: Specifies the appliance connection type to Db2.

OS User
: Specifies the original operator user ID that is used to connect to Db2.

DB User
: Specifies the primary AUTHID that is used for authorization within Db2. In most situations, this value is the same as OS User.

App. User (PROG=*program*)
: Specifies a valid DB2 program name, such as `DSNTEP2`.

App. User (PLAN=*plan*)
: Specifies a valid DB2 plan name, such as `DSNTEP2`.

Client Info (APPL=*transaction name*)
: Specifies a valid program (or user workstation transaction) name, such as `db2.exe`.

Client Info (WKSTN=*workstation name*)
: Specifies a valid user workstation name, such as `PCsys1`.

Client Info (USER=*user name*)
: Specifies a valid user name, such as `PCuser1`.

Object type (%/SYSIBM.SYSTABLE)
: Specifies a table.

These fields can be fully qualified, or partially qualified by using the percent sign wildcard character. For more information about using wildcard characters, see Filter wildcard support.
The most efficient CPU usage is achieved when you create a filter that eliminates the greatest number of events. To increase filtering efficiency, refine your filtering criteria by indicating the additional filtering types with specific values that are associated with the data that you want to collect.

Improving filtering efficiency

You can improve the CPU efficiency of filtering by including filter types in the filter. Specifying the plan, auth ID, connection type, operator ID, program, workstation user, workstation name, or object filter types that are associated with the performed action improves efficiency, as shown in the following example.

Example

To capture access to a table called *MY.TABLE*, you could create the following filter:

Filter 1
Schema.Table equal to *MY.TABLE*

This filter causes IBM Guardium S-TAP for Db2 to capture only those events that access MY.TABLE.

To increase efficiency in this example, specify a filter field, such as plan, even if you are sure that plan is the only plan that accesses this table. To capture access to the table *MY.TABLE* for an application that runs under a specific plan, such as *MYPLAN*, the following is an example of a more efficient filter:

Filter 2
Plan equal to *MYPLAN*
Schema.Table equal to *MY.TABLE*

Specifying the plan results in only those events with the specified plan and object being streamed to appliance. Fewer events streamed to the appliance results in improved CPU usage.

- **Event types and filtering**
  The following table shows the correlation between the event type and filtering. You can define and manage filtering criteria by setting the Database Type to DB2 Collection Profile in the Guardium Policy Builder of the Guardium appliance interface.
- **Filtering by database name**
  IBM Guardium S-TAP for Db2 enables you to filter by database name. You can specify database name filters, on a per-rule basis, to be included in the SQL activity filters.
- **Filter wildcard support**
  When you are creating a filter, value strings can include the percent sign (%) as a wildcard character. The wildcard character (%) enables the collector to match strings without you having to provide all possible string values for a filter value.

Parent topic: Data collection

Event types and filtering

The following table shows the correlation between the event type and filtering. You can define and manage filtering criteria by setting the Database Type to DB2 Collection Profile in the Guardium® appliance interface.

If you enable collection of SELECT/UPDATE/INSERT/DELETE events, then the event collection is subjected to additional filtering. If you enable collection of event types other than SELECT/UPDATE/INSERT/DELETE, then the events are collected without being subjected to filtering.

Table 1. Event types and filtering

Event type	Subjected to filtering?
SELECT/UPDATE/INSERT/DELETE (SUID)	Yes
CREATE/ALTER/DROP	No
GRANT/REVOKE	No
SET CURRENT SQLID	No
DB2® COMMANDS	No
Db2 UTILITIES	No
FAILED LOGINS	No
NEGATIVE SQLCODEs	No
COMMIT/ROLLBACK	No
BINDS/REBINDS	No

Enabling the collection of specific event types

The active policy determines which event types are enabled for collection. If the event type is enabled within a rule for the active policy, it is enabled for all rules within the active policy.

An event that is enabled in Rule 1 is subjected to subsequent rule filters. The following is an example using ASC event type collection:

- Rule 1 contains an Object field value of `%/%.%`.
- Rule 1 contains AUTHID filtering for User 1.
- Rule 2 contains AUTHID filtering for User 2.
- SELECT/UPDATE/DELETE/INSERT/SET CURRENT USERID/CREATE/ALTER/DROP events are collected for all tables for both User 1 and User 2.

Tip: This example could be simplified by placing both AUTHIDs into a group within a single rule.
The following is an example using event type collection:

- Rule 1 contains the collection of Utility events.
- Rule 1 contains AUTHID filtering for User 1.
- Rule 2 does not contain the collection of Utility events, but it contains AUTHID filtering for User 2.
- All Utility events are collected because they are enabled for Rule 1.

This list describes how you can enable the collection of specific event types:

SELECT/UPDATE/INSERT/DELETE (SUID)
Enable collection by including any filter type or non-blank value in the Object field of the rule.
Two target records are reported for nested INSERT/UPDATE/DELETE events: SELECT, and either INSERT, UPDATE, or DELETE. All nested INSERT/UPDATE/DELETE events are considered Table Change events. If the table filter is set to collect only READ events, then these events are filtered out (not collected).
Wildcarding can be used within the Object field value, for example: `%/SYSIBM.SYSTABLES` or `%/%.%`.
CREATE/ALTER/DROP
Collection is automatically enabled by including any filter type or non-blank value in the Object field of the rule.
Wildcarding can be used within the Object field value, for example: `%/SYSIBM.SYSTABLES` or `%/%.%`.
GRANT/REVOKE
Enable collection through the GRANT/REVOKE command setting.

SET CURRENT SQLID
: Collection is automatically enabled by including any filter type or non-blank value in the Object field of the rule.
  Wildcarding can be used within the Object field value, for example: `%/SYSIBM.SYSTABLES` or `%/%.%`.

DB2 COMMANDS
: Enable collection through the DB2 Commands command setting.

DB2 UTILITIES
: Enable collection through the UTILITES command setting.

FAILED LOGINS
: Enable collection through the FAILED AUTHID CHANGES command setting.

NEGATIVE SQLCODES
: Enable collection through the presence of a negative SQLCODE list. Only one list is allowed per policy.
  SQLCODE collection can be added to an active collection policy. A policy that contains a single rule with only negative SQLCODES results in an inactive policy.

COMMIT/ROLLBACK
: Enable collection by adding COMMIT/ROLLBACK to the Guardium appliance policy.

Parent topic: Filtering

Filtering by database name

IBM Guardium S-TAP for Db2 enables you to filter by database name. You can specify database name filters, on a per-rule basis, to be included in the SQL activity filters.

The following operations are supported:

Included operations
: The event is audited if any of the objects are in any of the DBNAMEs.

Excluded operations
: If all of the objects are not in any of the DBNAMEs, then it is a considered a match.
  Example: All of the objects must be in one or more of the DBNAMEs for them to be excluded. If an object is from a DBNAME that is not in the list, then it is considered a match. If any database that is accessed by the query is not in the EXCLUDE DB list, then the query must be captured.

Wildcarding
: Filter values can include the percent sign (%) as a wildcard character.

Parent topic: Filtering

Filter wildcard support

When you are creating a filter, value strings can include the percent sign (%) as a wildcard character. The wildcard character (%) enables the collector to match strings without you having to provide all possible string values for a filter value.

Note: The use of wildcards in filters can potentially result in the collection of significant amounts of captured data.
Filtering fields can be fully qualified, or partially qualified, by using the percent sign wildcard character. You can insert the wildcard character (%) anywhere within the value string. The presence of the wildcard character (%) represents a string of zero of more characters. It can be embedded within a string in the following ways to achieve the following results:

%
: Matches all strings.

%*a*
: Matches all strings that end with the letter *a*, for example: *a*, *ba*, *cba*.

a%
: Matches all strings that start with the letter *a*, for example: *a*, *ab*, *abc*.

a%*a*
: Matches all strings the begin and end with the letter *a*, for example *a*, *aba*, *aca*.

Note: The wildcard character (%) cannot be used explicitly as part of the filter value.
Parent topic: Filtering

Policy pushdown

At startup, the IBM Guardium S-TAP for Db2 collector agent waits for a policy to be streamed (or pushed down) from the Guardium system before activating a collection. When the collector agent receives a policy, it inactivates the active collection (if a collection is active), updates the collection profile with the new policy, and then activates the collection policy.

The following processing occurs in the collector agent when a policy is received:

1. The new policy is compared to the currently active policy if the new policy contains one or more rules.
   a. If the policies are identical, no further processing is required.
   b. If the policies are not identical, the policy is written to DD:ADHPLCY (if defined) and it becomes the active collection policy.
2. If the new policy does not apply to this subsystem, processing continues without any changes. In this case, if there is an active policy, the collection continues to use it. If no policy is active, none is started.
3. If the new policy is inactive (contains no general audit settings, table or target definitions), the active policy is inactivated.

Policy persistence

For a policy to be pushed down, the z/OS collector agent requires connection to the Guardium appliance. If the z/OS collector agent is unable to connect to the appliance, the z/OS collector agent will read the policy from the ADHPLCY DD (if it is defined in the started task JCL). The z/OS collector agent will activate collection based on the policy that is read from the DD until a connection with the appliance is established. When the connection is established, the policy that is pushed down from the appliance replaces the policy that was read from the DD.

The file contents defined by the ADHPLCY DD contains the policy from the last successful policy pushdown from the appliance.

If ADHPLCY is defined, it must point to a data set that is allocated with a record format of fixed blocked (RECFM=FB) and a record length (LRECL) greater than or equal to 80.

Suggested ADHPLCY DD settings are as follows:

- Record format (RECFM): FB
- Record length (LRECL): 80
- Block size (BLCKSIZE): 3120
- Data set name type (DSNTYPE): LIBRARY
- Data set organization (DSORG): PO

The ADHPLCY data set should be allocated with a minimum of 50 primary tracks and 10 secondary tracks. The ADHPLCY data set can be sequential, PDS, or PDS/E. If you use PDS or PDS/E, the space requirements might need to be increased in relation to the number of members that are contained within the data set.

For more information about creating, activating, and inactivating policies from the Guardium system interface, see the how-to topics in the *Security Guardium V10.1.3* documentation in the IBM Knowledge Center.

For more information about using data sets, see the z/OS documentation in the IBM Knowledge Center, https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.1.0/com.ibm.zos.v2r1.idad400/toc.htm.

Parent topic: Data collection

Streaming audit data to multiple systems

Multistream mode enables S-TAP audit events to be sent to multiple connected appliances. You can enable multistreaming to up to 6 Guardium appliances (APPLIANCE_SERVER + APPLIANCE_SERVER_*n*, where *n* can be 1 - 5).

Multistream mode provides a mechanism for distributing a high-volume workload over multiple connected appliances. In multistream mode, a single audit event is only sent to a single appliance. Multistream mode does not enable mirroring of the same set of audit events to multiple appliances.

IBM Guardium S-TAP for Db2 sends events to a single appliance until a ping occurs, or the number of records that is specified by MEGABUFFER_COUNT is reached.

To enable multistreaming, you must specify *MULTI_STREAM* when you configure the APPLIANCE_SERVER_LIST parameter. Parameters APPLIANCE_SERVER and APPLIANCE_SERVER_[1-5] specify the appliances to which you intend to stream events. The appliance that is specified by APPLIANCE_SERVER provides the policy that is used for event matching.

The APPLIANCE_SERVER parameter specifies the first appliance to which audit events are streamed. The collection policy that is pushed down from the first appliance determines which events are collected and streamed to all appliances that are enabled for multistreaming.

The IBM Guardium S-TAP for Db2 agent streams events to the first appliance, then sequentially to each subsequent appliance in the multistreaming set. Each appliance in the multistreaming set then processes (logs and discards) each event in accordance with the locally installed policies.

Parent topic: Data collection

Starting and stopping the collector agent

After you configure the product and review the data collection information, you can start the collector agent. Use the commands provided to start and stop the collector agent started task from a cataloged procedure library.

Procedure

1. To start the collector agent, use the START command.
   Example: /S ADHCSSID
2. To stop the collector agent, use the STOP command, or the MODIFY command with the STOP parameter.
   Example:

   ```
   /P ADHCSSID
   ```

   or

   ```
   /F ADHCSSID,STOP
   ```

Parent topic: Data collection

Including or excluding failed accesses and negative SQL code

IBM® Guardium® S-TAP® for DB2® enables you to include or exclude failed accesses and negative SQL code on a per-policy basis.

In the Guardium appliance interface, create a list of SQL codes to include of exclude during data collection. A policy can contain either all values to be included, or all values to be excluded. In an *include* list, any SQL activity that fails within the SQLCODE list will be collected. In an *exclude* list, any SQL activity that does not fail within the SQLCODE list will be collected.
Note:

- No other filtering criteria will be ANDed with the SQLCODE filter rule when determining the collection status of the event.
- Enabling AUDIT TRACE CLASS 1 (collection of failed accesses) is deprecated because negative SQL codes for these failed accesses will be collected.
- Failed access events are streamed to the appliance if the negative SQL code is:
  - Included in the list of negative SQLCODE to be captured
  - Not based on *ALL FAILED AUTHORIZATIONS* being included in the COMMANDS filter setting for the policy. *ALL FAILED AUTHORIZATIONS* can be removed from the COMMANDS filter setting.

Parent topic: Data collection

Quarantining SQL activity

IBM® Guardium® S-TAP® for DB2® enables you to quarantine the SQL activity of specific users for specific periods of time.

Quarantining a user of a specific Db2 subsystem means that for the period of time that is specified, the quarantined user will not be able to run SQL statement in the targeted Db2 subsystem. If a quarantined user attempts access during a restricted time, access will be denied. Use the Guardium appliance interface to quarantine user activity.

Note: Quarantine does not take effect immediately. The SQL statement that produces the event to trigger the quarantine is completed before the quarantine takes effect. It is possible for additional SQL statements to be run by the quarantined user before the quarantine takes effect.
Parent topic: Data collection

SQL Blocking

You can block the SQL activity of DB2® users' (Auth IDs) access to specific tables and databases. SQL statements that are run against accelerated tables are eligible for blocking if the blocking filtering criteria is met. If a SQL statement matches the blocking criteria, the SQL statement is prevented from running. Use the Guardium® appliance interface to define blocking policies.

Enabling blocking policy

Blocking policy pushdown maps blocking policies to the S-TAP® blocking mechanism within the collector agent. At startup, the collector agent checks if a blocking policy was streamed (or pushed down) from the IBM® Guardium system when a collection policy was pushed. When the collector agent receives a blocking policy, it inactivates any incidence of active blocking, updates the blocking policy, and activates blocking.

When a blocking policy is received, the collector agent completes the following steps:

1. Compares the new blocking policy to the currently active blocking policy, if the new policy contains one or more rules.
    - If the blocking policies are identical, the collector agent determines that no further processing is required.
    - If the blocking policies are different, then the new blocking policy replaces the old one.
2. Evaluates the pushed-down list and filters to determine which events to block.
3. Validates the list of supplied objects.
    - The object must exist at the time of the installation of the blocking policy.
    - If a table that is included in the blocking policy does not exist when the blocking policy is installed, message ADHP190W is generated to identify the table.
    - Blocking is not enabled for tables that are reported by a ADHP190W message.
    - The obid/dbid for the object are checked for performance reasons.
    - If the object is dropped and then recreated, the policy must be reinstalled.

If the field values of the SQL event match corresponding filter values (blocking rule conditions) in the blocking policy, then the SQL statements are blocked and ended with a -807 error code.

For more information about creating, activating, and inactivating blocking policies from the IBM Guardium system interface, refer to the Security Guardium documentation in the IBM Knowledge Center.

Enable or disable blocking on the host

If permitted, you can enable blocking, disable blocking, or report the blocking status (enabled or disabled) by using the following operator commands:

- /F <adhstc>,BLOCKING ENABLE
- /F <adhstc>,BLOCKING DISABLE
- /F <adhstc>,BLOCKING STATUS

These commands override and determine the blocking status whether or not a blocking policy is present. By default, blocking is enabled at startup; but if you use the /F <adhstc>,BLOCKING DISABLE command and push down blocking rules, the blocking rules will be processed and blocking will be established within the z/OS® agent, but blocking will not be enabled. If you use the /F <adhstc>,BLOCKING ENABLE command, blocking is not activated until a blocking policy is pushed down.

The ADHPARMS z/OS collector agent parameter, STAP_BLOCKING, controls whether the blocking operator command is permitted and whether blocking is enabled or disabled. For more information about STAP_BLOCKING, see Collector agent parameters.

Parent topic: Data collection

Controlling host variable collection

IBM® Guardium® S-TAP® for DB2® enables you to specify, on a per-rule basis, whether host variable information will be sent to the appliance for activity that matches that rule.

In the Guardium appliance interface, specify whether host variable information should be sent to the appliance for activity that matches a rule. When host variable collection is enabled, up to 256 bytes per variable of host variable data is sent to the Guardium appliance. For enhanced security of Personally Identifiable Information (PII), host variables are not collected by default in IBM Guardium S-TAP for Db2 V10.0 and later.

In the Guardium appliance interface, specify whether host variable information should be sent to the appliance for activity that matches a rule.

The Guardium appliance interface can be overridden by the FORCE_LOG_LIMITED parameter. This parameter enables you to restrict the collection of personal data by controlling whether the active policy controls the collection of host variables.

- If FORCE_LOG_LIMITED is set to *Y*, the policy setting for the collection of host variables is ignored, and host variables are not collected.
- If FORCE_LOG_LIMITED is set to *N*, the collection of host variables is controlled by the host variable settings in the active policy.

For more information, see Collector agent parameters.
Parent topic: Data collection

Collecting Command activity by using the Audit SQL Collector

IBM Guardium S-TAP for Db2 enables you to collect Command activity by using the Audit SQL Collector.

Command events are not subjected to filtering. All command events are streamed directly to the Guardium appliance for post-collection filtering. All command events are streamed directly to the Guardium appliance for optional post-collection filtering.

Parent topic: Data collection

Collecting SET CURRENT SQLID events by using the Audit SQL Collector

IBM Guardium S-TAP for Db2 V10.1.3 enables you to collect SET CURRENT SQLID events by using the Audit SQL Collector.

In IBM Guardium S-TAP for Db2 V10.1.3, IFI TRACE CLASS 7 is no longer enabled, and SET CURRENT SQLID events are automatically collected by using the Audit SQL Collector. SET CURRENT SQLID events are streamed to the Guardium appliance without being subjected to filtering.

Parent topic: Data collection

Reference information

These reference topics are designed to provide you with quick access to information about IBM Guardium S-TAP for Db2 sample library members, parameters, and variables.

Topics:

- Sample library members
- Collector agent parameters
- Collector agent sample parameter file
- ADHEMAC1 edit macro variables

Other resources

The following IBM documentation provides more information about configuring and operating this product.

- IBM Ported Tools for z/OS®: Open SSH User's Guide
- z/OS UNIX System Services Planning
- z/OS MVS™ JCL User's Guide
- Db2 Administration Guide
- Monitoring and Tuning Db2 Performance

- **Sample library members**
  Use the following sample library members that are included with IBM Guardium S-TAP for Db2 for installation and configuration.
- **MODIFY command**
  The MODIFY command allows you to issue requests against, and dynamically change, characteristics of an active S-TAP task.
- **Requesting and viewing S-TAP logging information**
  Use the S-TAP Logging command to issue a request for logging information from the S-TAP agent collector.
- **Collector agent parameters**
  The collector agent parameters are described in this section.
- **Keeping connections active when HOT_FAILOVER is enabled**
  When the HOT_FAILOVER feature is enabled by the APPLIANCE_SERVER_LIST parameter, all connection types (POLICY and ASC) for each connected Guardium appliance are kept active by pings.
- **Collector agent sample parameter file**
  The following sample parameter file is the minimum set of parameters required in a collector agent parameter file (ADHCFGP). If you want to use this sample file, verify that the values on each parameter are appropriate for your environment.
- **ADHEMAC1 edit macro variables**
  This table shows the ADHEMAC1 edit macro variables, including their default value and instructions for use. An example is also provided.

Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS

Sample library members

Use the following sample library members that are included with IBM Guardium S-TAP for Db2 for installation and configuration.

Table 1. Installation and configuration sample library members

Member	Type	Description
ADHBIND	JCL	Bind job used to bind DBRMs.
ADHBINDB	JCL	Bind job used to bind packages.
ADHCFGP	80-byte sequential or partitioned data set	A listing of required parameters that control how the collector is implemented.
ADHCFGPE	80-byte sequential or partitioned data set	A listing of optional parameters that control how the collector is implemented.
ADHCSSID	Procedure	IBM Guardium S-TAP for Db2 collector started task procedure. Runs an instance of the IBM Guardium S-TAP for Db2 collector started task.
ADHGRANT	JCL	Grants required authorizations to USERID and PLAN.

Member	Type	Description
ADHEMAC1	(edit macro)	Customizes the variables that appear in the DDL and JCL to be run.
ADHMSTR	JCL	Stops the IBM Guardium S-TAP for Db2 master address space.
ADHSJ000	JCL	Allocates VSAM product control file.
ADHSJ001	JCL	Sets product configuration options.
ADHSJ003	JCL	Generates the product control file content report.
ADHSTAPD	JCL	Produces an IBM Guardium S-TAP for Db2 diagnostic report.
ADHTCPD	JCL	Produces a TCP/IP diagnostic report to use for troubleshooting network connectivity and throughput issues.

Parent topic: Reference information

Related tasks

- Defining the collector agent started task JCL

MODIFY command

The MODIFY command allows you to issue requests against, and dynamically change, characteristics of an active S-TAP task.

The abbreviated version of the MODIFY command is the letter F. The general format of MODIFY is as follows:

```
>>-+-MODIFY-+--procname--,--parameter-------------------------><
   '-F------'
```

wherein:

procname
: The name of the member in a procedure library that was used to start the server or address space.

parameter
: Any of the parameters that are valid for the server.

S-TAP supported MODIFY options with descriptions

The following is a sample syntax diagram:

```
>>-+-MODIFY-+--procname,--+-STAP-+-----------------+
                          |      +-,HELP ----------|
                          |      +-,ALL-----------|
                          |      +-,POLICY--------|
                          |      +-,COUNTS--------|
                          |      +-,CONFIG--------|
                          |      +-,HISTORY_QUEUE--|
                          |      +-,HISTORY_FILTER-|
                          |      +-,HISTORY_IO-----|
                          |      +-,BLOCKING-------|
                          |      +-,QUARANTINE-----|
                          |      +-,GET_STATUS-----|
                          +-BLOCKING--+ ENABLED-----|
                          |           -+ DISABLED----|
                          |           -+ STATUS------|
                          |      +-,MUSTGATHER------|
                          |      +-,TRACE_POLICY,ENABLE----|
                          |      +-,TRACE_POLICY,DISABLE---|
                          |      +-,TRACE_COMPILE,ENABLE---|
                          |      +-,TRACE_COMPILE,DISABLE--|
                          |      +-,TRACE_PROTOBUF,ENABLE--|
                          |      +-,TRACE_PROTOBUF,DISABLE-|
                          |      +-,LOG_EVENTS,ENABLE------|
                          |      +-,LOG_EVENTS,DISABLE-----|
                          |      +-,LOG_LEVEL,F|I|W|E|S----|
                          |      +-,RESET_CONFIG-----------|
```

Note the space (rather than the comma) before BLOCKING ENABLED, DISABLED, and STATUS.
Options are defined as follows:

HELP
: Display all available commands

STAP
: Display the current status of the started task

ALL
: View all log information

POLICY
: View log information about the active policy

COUNTS
: View a log of detailed counts

CONFIG
: View a log about the current configuration

HISTORY_QUEUE

View log details about the internal events queue

HISTORY_FILTER
: View log information about event filter results

HISTORY_IO
: View log details about the streaming of events

BLOCKING
: View log information about the active blocking policy

QUARANTINE
: View log information about the active quarantine policy

GET STATUS
: Request the most recent count of events that were received/processed by the appliance

BLOCKING
: **ENABLED:** Enable the blocking feature. Blocking is activated if a blocking rule is pushed.
DISABLED: Disable the blocking feature.
STATUS: Display blocking status.

MUSTGATHER
: Send a must-gather request to the appliance

TRACE_POLICY,ENABLE
: View information about the policy component

TRACE_POLICY,DISABLE
: Hide information about the policy component

TRACE_COMPILE,ENABLE
: View information about the filter component

TRACE_COMPILE,DISABLE
: Hide information about the filer component

TRACE_PROTOBUF,ENABLE
: View information about the streaming component

TRACE_PROTOBUF,DISABLE
: Hide information about the streaming component

LOG_EVENTS,ENABLE
: Log events that are streamed to the appliance

LOG_EVENTS,DISABLE
: Hide events that are streamed to the appliance

LOG_LEVEL,F|I|W|E|S
: Control the amount of output log information that is generated by the agent: debugging, informational, warning, error, severe

RESET_CONFIG
: Reset agent configurations to the default settings

The following example displays the active S-TAP policy:

```
F ADHPROC,STAP,POLICY

ADHP110I  IBM Security Guardium DB2 S-TAP mode: STREAMING EVENTS
ADHP140I  Event Counts:
ADHP141I  CONNTYPE_OTHER (0) . . . . . . . . . . . 1
ADHP141I  CONNTYPE_TSO (1) . . . . . . . . . . . . 0
ADHP141I  CONNTYPE_CALL_ATTACH (2) . . . . . . . . 0
ADHP141I  CONNTYPE_DLI_BATCH (3)  . . . . . . . . 0
ADHP141I  CONNTYPE_CICS_ATTACH (4) . . . . . . . . 0
ADHP141I  CONNTYPE_IMS_ATTACH_BMP (5)  . . . . . . 0
ADHP141I  CONNTYPE_IMS_ATTACH_MPP (6)  . . . . . . 0
ADHP141I  CONNTYPE_DB2_PRIVATE_PROTOCOL (7)  . . 0
ADHP141I  CONNTYPE_DRDA_PROTOCOL (8) . . . . . . . 0
ADHP141I  CONNTYPE_IMS_CONTROL_REGION (9)  . . . 0
ADHP141I  CONNTYPE_IMS_TRANSACTION_BMP (10)  . . 0
ADHP141I  CONNTYPE_DB2_UTILITIES (11)  . . . . . 0
ADHP141I  CONNTYPE_RRSAF (12)  . . . . . . . . . 0
ADHP142I  MISC sent  . . . . . . . . . . . . . . 0
ADHP142I  UTILITY sent . . . . . . . . . . . . . 0
ADHP142I  DB2 COMMAND sent . . . . . . . . . . . 1
ADHP142I  SELECT sent  . . . . . . . . . . . . . 0
ADHP142I  UPDATE sent  . . . . . . . . . . . . . 0
ADHP142I  DELETE sent  . . . . . . . . . . . . . 0
ADHP142I  INSERT sent  . . . . . . . . . . . . . 0
ADHP142I  REVOKE sent  . . . . . . . . . . . . . 0
ADHP142I  GRANT sent   . . . . . . . . . . . . . 0
ADHP142I  COMMIT-ROLLBACK sent   . . . . . . . . 0
ADHP142I  BIND-REBIND sent   . . . . . . . . . . 0
ADHP142I  FAILED_SQLCODE sent   . . . . . . . .  0
ADHP143I  ALTER sent   . . . . . . . . . . . . . 0
ADHP143I  DROP sent  . . . . . . . . . . . . . . 0
ADHP143I  CREATE sent  . . . . . . . . . . . . . 0
ADHP144I  Bytes sent   . . . . . . . . . . . . . 363
ADHP145I  Events Sent  . . . . . . . . . . . . . 1
ADHP146I  Statements processed   . . . . . . . . 0
ADHP140I  Event Counts:
ADHQ3270I STAP INFO: STAGE1 FILTER IS.............. ACTIVE
ADHQ3270I STAP INFO: STAGE2 FILTER IS.............. NOTACTIV
ADHQ3270I STAP INFO: TOTAL EXEC SQL CALLS SEEN..... 0000000000000000
ADHQ3270I STAP INFO: STMTS PASSED STAGE1 FILTER....  0000000000000000
ADHQ3270I STAP INFO: STMTS FAILED STAGE1 FILTER....  0000000000000000
ADHQ3270I STAP INFO: STMTS PASSED, STAGE1 BYPASSED.  0000000000000000
ADHQ3270I STAP INFO: AUDS BLOCKS QUEUED............. 0000000000000000
ADHQ3270I STAP INFO: AUDS BLOCKS SENT TO APPLIANCE.. 0000000000000001
ADHQ3270I STAP INFO: AUDS BLOCKS NOT SENT TO APPL... 0000000000000000
ADHQ3270I STAP INFO: AUDS BLOCKS FREED ............. 0000000000000000
ADHQ3270I STAP INFO: AUDS BLOCKS FREED LOST ........ 0000000000000000
ADHQ3270I STAP INFO: BYTES SENT..................... 000000000000016B
```

```
ADHQ3270I STAP INFO: UTILITY EVENTS QUEUED.......... 0000000000000000
ADHQ3270I STAP INFO: UTILITY EVENTS FREED........... 0000000000000000
ADHQ3270I STAP INFO: UTILITY REQ COUNT.............. 0000000000000000
```

The following example displays the S-TAP blocking status:

```
F ADHPROC,STAP,POLICY

ADHQ9899I - BLOCKING STATUS
ADHQ2023I - AUTHID BLOCKING IS ENABLED
ADHQ2034I - BLOCK TABLE 181_9901F000 HASH TABLES 181_99101000 SQLHS 1E8B6000

<policy>
    <selectblocking-rule>
        <target>
            <schema>DBTROS</schema>
            <name>TABLE1</name>
        </target>
        <target>
            <schema>DBTROS</schema>
            <name>TABLE2</name>
        </target>
    </selectblocking-rule>
</policy>
```

The following example displays the results of S_TAP GET_STATUS:

```
F ADHPROC,STAP,GET STATUS
ADHP170I - Event count reported by the appliance at time: 112
```

Parent topic: Reference information

Requesting and viewing S-TAP logging information

Use the S-TAP Logging command to issue a request for logging information from the S-TAP agent collector.

About this task

From the S-TAP control panel of the IBM® Guardium® system interface:

Procedure

1. Locate the policy component for your S-TAP (for example, RS22:A91A:POLICY) and select the G icon.
2. Select STAP Logging for Command.
3. Select a logging level and click Apply to request S-TAP logging.
   S-TAP logging levels provide log information as follows:

   Level 0
   : Logs program levels, event queue statistics, agent configuration, policy, and event counts.

   Level 1
   : Logs agent configuration, policy, and event counts.

   Level 2
   : Logs agent configuration.

   Level 3
   : Logs policy.

   Level 4 or higher
   : Logs event counts.

4. To view the S-TAP logging information, locate the policy component of your S-TAP and click the i icon.

Parent topic: Reference information

Collector agent parameters

The collector agent parameters are described in this section.

APPLIANCE_CONNECT_RETRY_COUNT

Required: No

Default: 0

Description: The number of consecutive failed connection attempts before terminating. The value of 0 indicates to never stop attempting connections. A value of 1 indicates a stop immediately after connection attempt fails. Range: 0 - 99999.

Syntax:

APPLIANCE_CONNECT_RETRY_COUNT*(retry_count)*

Example:

```
APPLIANCE_CONNECT_RETRY_COUNT(1000)
```

APPLIANCE_NETWORK_REQUEST_TIMEOUT

Default: 0

Range: 0 or 500 - 12000

Description: The value in milliseconds of the period of time to wait for network communication request send or receive to complete. A value of 0 results in no timeout period.

Syntax:

```
APPLIANCE_NETWORK_REQUEST_TIMEOUT(timeout)
```

Example:

```
APPLIANCE_NETWORK_REQUEST_TIMEOUT(0)
```

APPLIANCE_PING_RATE

Required: No

Default: 5

Description: Specifies the time interval between accesses to the Guardium system to prevent timeouts (disconnects) during idle periods. The value is in number of seconds.

Syntax:

```
APPLIANCE_PING_RATE(ping_interval)
```

Example:

```
APPLIANCE_PING_RATE(5)
```

APPLIANCE_PORT

Required: No

Default: 16022

Valid ports: 16022 or 16023

Description: The IP port number of the Guardium system to which the IBM Guardium S-TAP for Db2 audit data collector should connect. This parameter must be properly configured to enable collection of audit data and a connection to the IBM Guardium system. If port 16023 is used, encryption support is required for the connection to the appliance.

Note: Specifying this keyword and parameter designates the port on which the Guardium appliance is listening to the S-TAP. The port is dedicated to the IP address of the appliance. Port 16022 or 16023 can also be in use on z/OS® by another application.

Syntax:

```
APPLIANCE_PORT(port_number)
```

Example:

```
APPLIANCE_PORT(16022)
```

APPLIANCE_RETRY_INTERVAL

Required: No

Default: 3

Description: Specifies the time interval between attempts to establish a connection to the IBM Guardium system. The value is in number of seconds.

Syntax:

```
APPLIANCE_RETRY_INTERVAL(retry_interval)
```

Example:

```
APPLIANCE_RETRY_INTERVAL(3)
```

APPLIANCE_SERVER

Required: Yes

Default: None

Description: The host name or IP address (in dotted-decimal notation, for example: 1.2.3.4) of the IBM Guardium system to which the IBM Guardium S-TAP for Db2 audit data collector should connect.

Note: This parameter must be properly configured to enable collection of audit data, and a connection to the IBM Guardium system. The value can contain up to 128 characters.

Syntax:

```
APPLIANCE_SERVER(hostname|ip_address)
```

Example:

```
APPLIANCE_SERVER(192.168.2.205)
```

APPLIANCE_SERVER_FAILOVER_[1-5]

Required: No

Default: None

Description: The host name or IP address (in dotted-decimal notation, for example: 1.2.3.4) of the IBM Guardium system to which the IBM Guardium S-TAP for Db2 audit data collector should fail over to if APPLIANCE_SERVER is not available.

Note:

1. This parameter must be properly configured to enable collection of audit data and a connection to the IBM Guardium system. The value can contain up to 128 characters.
2. The collector agent attempts to connect to the fail over systems beginning with APPLIANCE_SERVER_FAILOVER_1, and ending with APPLIANCE_SERVER_FAILOVER_5.
3. Both the APPLIANCE _SERVER_FAILOVER_[1-5] and APPLIANCE_SERVER_[1-5] parameters can be used to designate servers for multistreaming or failover. Use the APPLIANCE_SERVER_LIST(MULTI_STREAM|FAILOVER) parameter to designate how these parameters are used.

Syntax:

```
APPLIANCE_SERVER_FAILOVER_1(hostname|ip_address)
```

Example parameter settings to enable multistream support:

```
APPLIANCE_SERVER_LIST(MULTI_STREAM)
APPLIANCE_SERVER(guardium1.company.com)
APPLIANCE_SERVER_1(guardium2.company.com)
APPLIANCE_SERVER_2(guardium3.company.com
```

APPLIANCE_SERVER_LIST(FAILOVER|MULTI_STREAM|HOT_FAILOVER)

Required: No

Default: FAILOVER

Description: If set to MULTI_STREAM, this parameter specifies that a Guardium appliance connection is to be established for each server that is identified by the APPLIANCE_SERVER_n parameter.

- If a connection is lost, S-TAP audit events continue to transmit over the remaining appliance connection.
- Lost connections are retried at regular intervals that are determined by multiplying the APPLIANCE_CONNECT_RETRY_COUNT by the APPLIANCE_PING_RATE.

If set to FAILOVER, this parameter specifies that one Guardium appliance connection is to be active at a time.

- If the connection to the primary appliance is lost, a failover action occurs, which results in an attempt to connect to the next available server. The next available server is identified by the APPLIANCE_SERVER_FAILOVER_n parameter.
- After a failover action occurs, the connection to the primary server is retried at regular intervals that are determined by multiplying the APPLIANCE_CONNECT_RETRY_COUNT by the APPLIANCE_PING_RATE.

With either setting of APPLIANCE_SERVER_LIST, if all connections fail, and a spill file is specified (parameter OUTAGE_SPILLAREA_SIZE), events are buffered to the spill file until a connection becomes available. If no spill file is specified, and all connections are lost, data loss occurs.

If set to HOT_FAILOVER, this parameter causes all connection types (POLICY and ASC) for each connected Guardium appliance to be kept active by pings. You can specify the primary Guardium appliance by using the APPLIANCE_SERVER parameter. If the primary Guardium appliance becomes unavailable and failover occurs, HOT_FAILOVER maintains the activity of the primary appliance policy.

Syntax:

```
APPLIANCE_SERVER_LIST_FAILOVER
```

Example:

```
APPLIANCE_SERVER_LIST_FAILOVER
```

AUDIT

Required: Yes

Default: None

Description: The Db2 subsystem ID for the Db2 subsystem on which the IBM Guardium S-TAP for Db2 Collector Agent should capture query data.

Note: This parameter must be properly configured to enable collection of capture data. The value can contain up to 4 characters.
Syntax:

```
AUDIT(ssid)
```

Example:

```
AUDIT(DSN1)
```

AUTHID

Required: No

Default: Defaults to the user ID under which the started task will run.

Description: The AUTHID parameter defines the Db2 AUTHID that IBM Guardium S-TAP for Db2 uses when establishing a connection to Db2 during interval processing. If you are using RACF® on your Db2 system, this ID must be defined to RACF. The AUTHID specified needs to be authorized through the resident security package, such as RACF, to perform the functions needed for all processes done by the started task and the Collector Agent monitoring subsystem. Such processes include connecting to each of the monitored Db2 SSIDs and performing file update activities against the IBM Guardium S-TAP for Db2 VSAM control file.

Notes:

1. The ID specified in the startup parameter AUTHID must be a valid TSO user ID and not a RACF group name.

2. If the AUTHID parameter is defined in the RACF Started Procedures Table (ICHRIN03), it should not be used as a startup parameter. The Started Procedures Table (ICHRIN03) associates the names of started procedures with specific RACF user IDs and group names. It can also contain a generic entry that assigns a user ID or group name to any started task that does not have a matching entry in the table. However, it is recommended that you use the STARTED class for most cases rather than the started procedures table.

Syntax:

```
AUTHID(db2authid)
```

Where *db2authid* is the Db2 AUTHID that IBM Guardium S-TAP for Db2 uses when establishing a connection to Db2 during interval processing.
Example:

```
AUTHID(DB2USER)
```

CICS_USERID

Required: No

Default: N

Description: If set to Y, the CICS_USERID parameter enables the capture of CICS Login User ID for SQL statements that are run in Db2 for CICS. For more information see Enabling CICS Login User ID reporting.

Syntax:

```
CICS_USERID(YES|NO)
```

Example:

```
CICS_USERID(Y)
```

COLLECT_COMMIT_ROLLBACK

Required: No

Default: N

Description: If set to Y, the COLLECT_COMMIT_ROLLBACK parameter enables the collection of COMMIT and ROLLBACK events.

Syntax:

```
COLLECT_COMMIT_ROLLBACK(YES|NO)
```

Example:

```
COLLECT_COMMIT_ROLLBACK(Y)
```

DEBUG

Required: No

Default: N

Description: The DEBUG parameter turns on debug mode and produces diagnostic messages for use by IBM Software Support.

Syntax:

```
DEBUG(YES|NO)
```

Example:

```
DEBUG(Y)
```

FORCE

Required: No

Default: N

Description: The FORCE parameter forces installation of a monitoring agent. If you use this parameter, any return codes from any failure reported in message ADHQ2002E are overridden.
Note: This parameter should not be specified without instruction by IBM Software Support.
Syntax:

```
FORCE(YES|NO)
```

Example:

```
FORCE(Y)
```

FORCE_LOG_LIMITED

Required: No

Default: N

Description: This parameter enables you to restrict the collection of sensitive data by controlling whether the active policy controls the collection of host variables.

If this parameter is set to *Y*:

- The policy setting for collection of host variables is ignored and host variables are not collected.

- The APPLIANCE_PORT parameter must be set to 16023. Port 16023 is used for AT-TLS-configured encrypted communications. If APPLIANCE_PORT is not set to 16023, the S-TAP agent will generate a log message indicating the configuration inconsistency, and shut down.

If this parameter is set to *N*, the collection of host variables is controlled by the host variable settings in the active policy.

Syntax:

```
FORCE_LOG_LIMITED(YES|NO)
```

Example:

```
FORCE_LOG_LIMITED(Y)
```

HOSTVAR_LIMIT

Required: No

Default: 1500

Description: This parameter designates the number of storage blocks to be allocated for host variable collection per event. The valid range is 1 -- 9999. If this parameter is not customized, the default value of 1500 is set.

If error message ADHQ1203I is encountered with RC=0008 and RSN=003F, increase the HOSTVAR_LIMIT setting to accommodate the collection of host variables for the monitored workload.

If IBM Guardium S-TAP for Db2 and IBM Db2 Query Monitor for z/OS are simultaneously monitoring the same Db2 subsystem, both products must have matching HOSTVAR_LIMIT settings to avoid receiving a mismatch error.

Syntax:

```
HOSTVAR_LIMIT(n)
```

where *n* is an integer between 1 - 9999.
Example:

```
HOSTVAR_LIMIT(1500)
```

ISM_CONSTRAINT_AGE

Required: No

Default: 300

Description: This parameter controls how much time must have passed since the last storage constraint occurrence for a given ISM storage space before the constraint event is considered to have been relieved.

Syntax:

```
ISM_CONSTRAINT_AGE(n)
```

where *n* is an integer between 1 - 60000 specified in .01 seconds. The default value is 300.
Example:

```
ISM_CONSTRAINT_AGE(16)
```

ISM_ERROR_DETAIL

Required: No

Default: Y

Description: This parameter controls whether messages ADHQ1203I and ADHQ1204I are issued to provide detailed information for ISM Storage Constraint situations. The product recommendation is to leave this parameter set to Y. This setting can be overridden at run time with the /f cqmstc,ISMERROR_DETAIL command.

Syntax:

```
ISM_ERROR_DETAIL(Y|N)
```

Example:

```
ISM_ERROR_DETAIL(Y)
```

ISM_ERROR_BLOCKS

Required: No

Default: 256

Description: This parameter determines the number of ISM Error Blocks that are allocated when IBM Guardium S-TAP for Db2 initializes.

If this value is too low, message ADHQ1219W might be issued. ISM Error Blocks communicate a storage constraint event from somewhere in the product to the task that issues storage constraint messages. If you run out of ISM Error Blocks, the storage constraint message will not be issued. However, an abend table entry will be created to document this event. This is most likely a temporary situation and it does not impact the overall performance of IBM Guardium S-TAP for Db2.

Syntax:

```
ISM_ERROR_BLOCKS(n)
```

where *n* is an integer, 16 - 8192. The default value is 256.
Example:

```
ISM_ERROR_BLOCKS(256)
```

ISM_ERROR_MSG_BLOCKS

Required: No

Default: 256

Description: This parameter determines the number of ISM Error Message Blocks that are allocated when IBM Guardium S-TAP for Db2 initializes. If this value is too low, duplicate ISM error message can be issued for the same space and reason instead of incrementing the occurrence count.

ISM Error Message Blocks are used by the task that issues storage constraint messages to do two things:

1. To consolidate similar storage constraint events to eliminate duplicate messaging for the same condition, and
2. To keep track of storage constraint events so that the Storage Constraint Relieved situation can be detected and messaged.

If you run out of ISM Error Message Blocks, this consolidation will not always occur. This would result in additional, duplicate messages in the log for the similar storage constraint events.

Syntax:

```
ISM_ERROR_MSG_BLOCKS(n)
```

where *n* is an integer between 16 - 8192. The default value is 256.
Example:

```
ISM_ERROR_MSG_BLOCKS(256)
```

MASTER_PROCNAME

Required: Yes

Default: None.

Description: The MASTER_PROCNAME parameter enables users to specify the PROCNAME to be used for the Master Address Space. Specifying this parameter causes IBM Guardium S-TAP for Db2 to use the Master Address Space with the same name.

- The MASTER_PROCNAME for IBM Guardium S-TAP for Db2 and Query Monitor must be the same when each is started at the same time for the same Db2 Subsystem.
- If this Master Address Space is already started, it is shared with other IBM Guardium S-TAP for Db2 subsystems that are already using it.
- If this Master Address Space has not already been started, it will start automatically.

Syntax:

```
MASTER_PROCNAME(procname)
```

where *procname* is the specified Master Address Space PROCNAME (character, 8 bytes).)
Example:

```
MASTER_PROCNAME(CQMMASTR)
```

MAXIMUM_ALLOCATIONS

Required: No

Default: 2048

Description: This parameter determines the maximum amount of global shared memory to be allocated by IBM Guardium S-TAP for Db2 for internal Integrated Storage Manager spaces.

Syntax:

```
MAXIMUM_ALLOCATIONS(n)
```

where *n* is an integer between 512 - 32768 specified in megabytes; must be smaller than SMEM_SIZE.
Example:

```
MAXIMUM_ALLOCATIONS(2048)
```

MESSAGE_LOG_LEVEL

Required: No

Default: I

Description: Controls the amount of output log information that is generated by the agent:

I
: Includes all log messages with an *informational* severity or higher

W
: Includes all log messages with a *warning* severity or higher

E
: Includes all log messages with an *error* severity or higher

S
: Includes all log messages with a *severe* severity or higher

The ADHPARMS file is read when the agent is started. Modifying the log-level setting in the ADHPARMS file does not implement the new setting until you restart the collector agent.
Note: During installation, it is recommended that you set the MESSAGE_LOG_LEVEL to I.

Syntax:

```
MESSAGE_LOG_LEVEL(I|W|E|S)
```

Example:

```
MESSAGE_LOG_LEVEL(I)
```

OUTAGE_SPILLAREA_SIZE

Required: No

Default: 0

Description: This parameter determines the maximum amount of memory to be allocated to support the retention of audit data in the event of a Guardium system connection outage.
Note: A value of 0 disables spillfile support. When enabled, OUTAGE_SPILLAREA_SIZE supersedes SEND_FAIL_EVENT_COUNT for temporary data retention.
Syntax:

```
OUTAGE_SPILLAREA_SIZE(n)
```

where *n* is an integer between 0 - 1024 specified in megabytes.
Example:

```
OUTAGE_SPILLAREA_SIZE(2)
```

PREFER_IPV4_STACK

Required: No

Default: N

Description: If set to Y, this parameter causes a request to be issued to the Domain Name Server (DNS) for an IPV4 address for the hostname that is specified in the APPLIANCE_SERVER parameter:

- The DNS lookup request for an IPV4 address is attempted. If an IPV4 address is defined for the hostname, the DNS will respond with the value that will be used to connect to the Guardium appliance.
- If only an IPV6 address is defined at the DNS, then the DNS will respond with the IPV6 address that will be used to connect to the Guardium appliance.
- If both IPV4 and IPV6 addresses are defined at the Guardium appliance, the DNS will respond with both addresses, and the IPV4 address will be used to connect to the appliance.

If this parameter is set to N or omitted from configuration, a request for an IPV6 address is issued to the DNS for the hostname that is specified by the APPLIANCE_SERVER parameter:

- The DNS lookup request for an IPV6 address is attempted. If an IPV6 address is defined for the hostname, the DNS will respond with the value that will be used to connect to the Guardium appliance.
- If only an IPV4 address is defined at the DNS, then the DNS will respond with the IPV4 address that will be used to connect to the Guardium appliance.
- If both IPV4 and IPV6 addresses are defined at the Guardium appliance, the DNS will respond with both addresses, and the IPV4 address will be used to connect to the appliance.

Note: Whether or not this parameter is used, if the address returned from the DNS is not valid for the hostname, it will result in failure to connect to the appliance, and the IBM Guardium S-TAP for Db2 started task will terminate.
Syntax:

```
PREFER_IPV4_STACK(Y|N)
```

Example:

```
PREFER_IVP4_STACK(Y)
```

SEND_FAIL_EVENT_COUNT

Required: No

Default: 100

Description: Specifies the maximum number of events to be buffered during a communication outage with the Guardium system. Events are buffered in internal memory objects and streamed to the appliance at the time of reconnection.
Note: SEND_FAIL_EVENT_COUNT and OUTAGE_SPILLAREA_SIZE are mutually exclusive. When OUTAGE_SPILLAREA_SIZE is specified, spillfile support is enabled, which supersedes SEND_FAIL_EVENT_COUNT for temporary data retention.
Syntax:

```
SEND_FAIL_EVENT_COUNT (event_count)
```

where *event_count* is an integer between 0 – 1024 that represents the number of events to be buffered.
Example:

```
SEND_FAIL_EVENT_COUNT(100)
```

SMEM_SIZE(5|n)

Required: No

Default: 5

Description: This parameter determines the maximum amount global shared memory to be allocated by IBM Guardium S-TAP for Db2 for all purposes.

Syntax:

```
SMEM_SIZE(n)
```

where *n* is an integer between 3 - 32 specified in gigabytes; must be three times larger than MAXIMUM_ALLOCATIONS.
Example:

```
SMEM_SIZE(5)
```

STAP_BLOCKING

Required: No
Default: ENABLED
Description: The STAP_BLOCKING parameter controls whether blocking is enabled or disabled and whether the blocking operator command is permitted to enable, disable, or report status for blocking. This parameter cannot be overwritten by the BLOCKING operator command. STAP_BLOCKING parameter options are as follows:

- STAP_BLOCKING(ENABLED) enables the blocking feature. Blocking is activated if a blocking rule is pushed.
- STAP_BLOCKING(DISABLED) disables the blocking feature.
- STAP_BLOCKING(OPERATOR) enables the blocking feature and enables the BLOCKING operator command. Blocking is activated if a blocking rule is pushed.

Syntax: STAP_BLOCKING(ENABLED|DISABLED|OPERATOR)
Example: STAP_BLOCKING(ENABLED)

STAP_MEGABUFFER

Required: No

Default: Y

Description: When multiple IBM Guardium S-TAP for Db2 audit events are accumulated in a buffer, it is referred to as a megabuffer. A megabuffer reduces the CPU usage that is related to TCP/IP activity. To optimize IBM Guardium S-TAP for Db2 performance, STAP_MEGABUFFER must remain set to `Y`. However, STAP_MEGABUFFER can be set to `N` when buffering is not desired.

Setting the STAP_MEGABUFFER parameter to `N` eliminates buffering, and provides near real-time event streaming to the Guardium appliance. It also increases CPU usage, due to additional TCP/IP calls.

Syntax:

```
STAP_MEGABUFFER(Y|N)
```

Example:

```
STAP_MEGABUFFER(Y)
```

STAP_STREAM_EVENTS

Required: No

Default: Y

Description: This parameter specifies whether events will be streamed to the IBM Guardium system. The default value, *Y*, enables streaming. Specify *N* to disable streaming and enable Simulation mode.

Syntax:

```
STAP_STREAM_EVENTS(Y|N)
```

Example:

```
STAP_STREAM_EVENTS(Y)
```

STAP_TERMINATE_OPTIMIZE

Required: No

Default: N

Description: This parameter can be used to improve the response time for processing STAP_TERMINATE requests from the Guardium appliance. Roundtrip time for STAP_TERMINATE activity is impacted by the STAP_MEGABUFFER parameter. STAP_TERMINATE policies require near real-time event recording to the IBM Guardium system to analyze events against the policy and issue the termination requests to IBM Guardium S-TAP for Db2. To enable near real-time event recording to the Guardium appliance, set the STAP_MEGABUFFER parameter to `N`.

Syntax:

```
STAP_TERMINATE_OPTIMIZE(Y|N)
```

Example:

```
STAP_TERMINATE_OPTIMIZE(N)
```

STAP_UTILITY_MULTITABLE

Required: No

Default: N

Description: The STAP_UTILITY_MULTITABLE parameter works in conjunction with the STAP_UTILITY_TS_TO_TABLE parameter. These parameters control how table information is reported for Db2 Utility access events that involve tablespaces. The STAP_UTILITY_MULTITABLE parameter controls the behavior of the collector when multiple tables are contained in the tablespace. When STAP_UTILITY_MULTITABLE is set to Y:

- The collector will report all tables in the tablespace that are impacted by the utility. This guarantees that tablespace access by a utility execution will result in an audit event against the table name.
- Tables within a tablespace, which were not accessed by the utility, might be reported.

When STAP_UTILITY_MULTITABLE is set to N, no attempt is made to report table information for multi-table tablespaces accessed by a utility. Only the tablespace name is reported.

Syntax:

```
STAP_UTILITY_MULTITABLE(Y|N)
```

Example:

```
STAP_UTILITY_MULTITABLE(N)
```

No table names are reported (default).

```
STAP_UTILITY_MULTITABLE(Y)
```

All table names are reported.

STAP_UTILITY_TS_TO_TABLE

Required: No

Default: Y

Description: The STAP_UTILITY_TS_TO_TABLE parameter controls how table information is reported for Db2 Utility accesses to tablespaces. When the parameter is set to Y, the collector queries the Db2 catalog. The collector then determines and reports on which table exists within the tablespace that has been accessed by the utility execution. If multiple tables are contained in the tablespace, the STAP_UTILITY_MULTITABLE parameter controls whether the collector reports either:

All tables
: All table names in the accessed tablespace

No tables
: Only the tablespace is reported.

This action is controlled by STAP_UTILITY_MULTITABLE parameter setting.

Syntax:

```
STAP_UTILITY_TS_TO_TABLE(Y|N)
```

Example:

```
STAP_UTILITY_TS_TO_TABLE(Y)
```

STARTUP_DIAGNOSTICS

Required: No

Default: N

Description: The STARTUP_DIAGNOSTICS parameter causes IBM Guardium S-TAP for Db2 to produce diagnostic information output during startup of the collector agent. This output might be useful to IBM Support when diagnosing reported problems.

Syntax:

```
STARTUP_DIAGNOSTICS(Y|N)
```

Example:

```
STARTUP_DIAGNOSTICS(Y)
```

SHUTDOWN_DIAGNOSTICS

Required: No

Default: N

Description: The SHUTDOWN_DIAGNOSTICS parameter causes IBM Guardium S-TAP for Db2 to produce diagnostic information output during shutdown (stop) of the collector agent. This output might be useful to IBM Support when diagnosing reported problems.

Syntax:

```
SHUTDOWN_DIAGNOSTICS(Y|N)
```

Example:

```
SHUTDOWN_DIAGNOSTICS(Y)
```

SUBSYS

Required: No

Default: The default value is the Db2 subsystem name.

Description: The SUBSYS parameter defines the SQL Collector subsystem name. The subsystem name does not need to correspond to a Db2 subsystem nor an MVS™ operating system name. The name must be 1-4 characters in length.

Syntax:

```
SUBSYS(ssid)
```

Where *ssid* is the 1-4 character SQL Collector subsystem name.
Note: The SQL Collector subsystem ID must be unique across the SYSPLEX. A SQL Collector component subsystem must be running on each LPAR that has a Db2 subsystem to be captured. When choosing a collector agent subsystem ID name, be sure it will not conflict with another on the SYSPLEX. If the specified SUBSYS is not unique across the SYSPLEX, message ADHQ1003E will be issued.

Example:

SUBSYS(ADH1)

TS_OFFSET(E|W.HH.MM)

Required: No

Default: None (no offset)

Description:

- This parameter enables you to adjust the event timestamps that are steamed to the appliance by specifying the amount of time to adjust (offset) based on timezone.
  - For example, if running with a clock that is set to UTC 0.0 in a timezone that it is UTC + 9, GMT can be considered 9 hours west of the current time. In this situation, the parameter should be set as follows: `TS_OFFSET(W.09.00)`. Event timestamps will be adjusted (offset) by subtracting 9 hours from the original timestamp.
- If TS_OFFSET is not supplied, the timestamps that are streamed to the appliance are not adjusted based on timezone.

Syntax:

E|W
: East or west offset from GMT

HH
: Number of hours

MM
: Number of minutes

Example: TS_OFFSET(W.09.00)

ZIIP_FILTER(Y|N)

Required: No

Default: ZIIP_FILTER(N)

Description:

- ZIIP_FILTER(Y) indicates that the z/OS image running the collector agent started task has an IBM System z® Integrated Information Processor (zIIP). In this case, allow collector agent to perform offload profile filtering to a zIIP.
- If ZIIP_FILTER(Y) is specified and the collector agent started task is running on a z/OS that has no zIIP, message ADHQ1060I is issued, indicating the WLM related service has failed. In this case, collector agent continues to run as if ZIIP_FILTER(N) were set.

Syntax:ZIIP_FILTER(Y)

Example:ZIIP_FILTER(Y)

ZIIP_TCP(Y|N)

Required: No

Default:ZIIP_TCP(N)

Description:

- ZIIP_TCP(Y) indicates that the z/OS image running the collector agent started task has an IBM System z Integrated Information Processor (zIIP). In this case, allow collector agent to offload TCP/IP message processing to a zIIP.
- If ZIIP_TCP(Y) is specified and the collector agent started task is running on a z/OS that has no zIIP, message ADHQ1060I is issued, indicating the WLM related service has failed. In this case, collector agent continues to run as if ZIIP_TCP(N) were set.
  Note: ZIIP_TCP(Y) requires that zIIP filter support be enabled: ZIIP_FILTER(Y). If ZIIP_FILTER(N) and ZIIP_TCP(Y) are specified together, ZIIP_FILTER will be automatically set to Y.

Syntax:ZIIP_TCP(Y)

Example:ZIIP_TCP(Y)

/f cqmstc,ISMERROR_DETAIL(Y|N)

Description: This parameter controls whether ISM constraint message detail is on or off. When the parameter is specified, messages ADHQ1203I and ADHQ1204I are issued for ISM storage constraint situations.

Parent topic: Reference information

Keeping connections active when HOT_FAILOVER is enabled

When the HOT_FAILOVER feature is enabled by the APPLIANCE_SERVER_LIST parameter, all connection types (POLICY and ASC) for each connected Guardium® appliance are kept active by pings.

If the primary appliance becomes unavailable and failover occurs, the appliance policy that was originally pushed from the primary appliance continues to be active. When all Guardium appliances are connected, the status of each appliance connection, listed in the Guardium interface, is green.

Parent topic: Reference information

Collector agent sample parameter file

The following sample parameter file is the minimum set of parameters required in a collector agent parameter file (ADHCFGP). If you want to use this sample file, verify that the values on each parameter are appropriate for your environment.

```
-  5655-STP
-  (C) COPYRIGHT ROCKET SOFTWARE, INC. 1999 - 2015 ALL RIGHTS RESERVED.
-
-  MEMBER: ADHCFGP
-
-  DESCRIPTION: THIS IS A SAMPLE MINIMUM ADHCFGP MEMBER
-               USED FOR IBM SECURITY GUARDIUM S-TAP for DB2 on z/OS
-               COLLECTOR AGENT STARTUP.
-               VERIFY THAT THE VALUES ON EACH PARM ARE APPROPRIATE
-               FOR YOUR ENVIRONMENT.
-
- NOTE:  AFTER USING THE EDIT MACRO, VERIFY THAT NONE OF THE
-        STATEMENTS EXCEED COLUMN 72 IN LENGTH.
-
-
SUBSYS(#SSID)              -
AUDIT(#SSID)              -
MASTER_PROCNAME(ADHMST31)  -
APPLIANCE_SERVER(#APPSRVR)
```

Parent topic: Reference information

ADHEMAC1 edit macro variables

This table shows the ADHEMAC1 edit macro variables, including their default value and instructions for use. An example is also provided.

Table 1. ADHEMAC1 Edit macro variables

Variable	Default	Instructions
#SSID	MYSSID	Change the default to a valid Db2 subsystem ID. Note: The ADHEMAC1 macro sets the SUBSYS parameter using the #SSID variable. Running the macro sets SUBSYS to the Db2 subsystem ID used by the collector agent task. Do not change the #SSID variable in the ADHEMAC1 macro to be anything other than the Db2 subsystem ID used by the collector agent task.
#ADHOWNER	&ZUSER	Change &ZUSER to the value of #ADHQUALIFIER. #ADHOWNER is used to configure the owner of the plans and packages. It is used as the owner value of objects created by statements contained within the package or plan.
#ADHQUALIFIER	SYSTOOLS	Change the default to the schema name being used with this product.
#ADHUSERID	&ZUSER	Use as the authorization ID for the collector agent task.
#SADHLOAD	ADH.IBMTAPE.SADHLOAD	Change the default to the data set containing the IBM Guardium S-TAP for Db2 load modules.
#SADHDBRM	ADH.IBMTAPE.SADHDBRM	Change the default to the data set containing the IBM Guardium S-TAP for Db2 DBRMs.
#SDSNLOAD	DSN.Vxxx.SDSNLOAD	Change the default to the data set containing the Db2 load modules.
#SDSNRUNL	DSN.Vxxx.RUNLIB.LOAD	Change the default to the data set containing the Db2 DSNTEP2 module.
#DSNTEP2	DSNTEP2	Change the default to the DSNTEP2 plan name.
ADHPLAN1	ADHPLAN1	Change the default to a valid plan name. This plan used to collect information about the Db2 System catalog during audit data collection.
#SZPARM	MYSSIDPARM	Change the default to the Db2 ZPARM member that is associated with the Db2 subsystem.
#SBSDS01	MYSSID.BSDS01	Change the default to the DSN of the bootstrap data set 01.
#SBSDS02	MYSSID.BSDS02	Change the default to the DSN of the bootstrap data set 02.
#SDSNEXIT	DSN.Vxxx.SDSNEXIT	Change the default to the data set containing the Db2 ZPARMs.
#SFECLOAD	None	Data set name of the required FEC load library.
#SCQCLOAD	None	Data set name of the required CQC load library.
#ADHCNTRLFILE	ADH.V0A00.CONTROL	Change the default to an appropriate DSN HLQ for the IBM Guardium S-TAP for Db2 VSAM Control file.
#APPSRVR	appliance.company.com	Host name or IP address of the IBM Guardium system.

The following example shows the contents of the ADHEMAC1 member:

```
ISREDIT MACRO (NP)
ISPEXEC VGET (ZUSER)
ISREDIT CHANGE ALL '#SSID'         MYSSID
```

```
ISREDIT CHANGE ALL '#ADHOWNER'     &ZUSER
ISREDIT CHANGE ALL '#ADHUSERID'    &ZUSER
ISREDIT CHANGE ALL '#SADHLOAD'     ADH.IBMTAPE.SADHLOAD
ISREDIT CHANGE ALL '#SADHDBRM'     ADH.IBMTAPE.SADHDBRM
ISREDIT CHANGE ALL '#SDSNLOAD'     DSN.Vxxx.SDSNLOAD
ISREDIT CHANGE ALL '#SDSNRUNL'     DSNxxx.RUNLIB.LOAD
ISREDIT CHANGE ALL '#DSNTEP2'      DSNTEP2
ISREDIT CHANGE ALL 'ADHPLAN1'      ADHPLAN1
ISREDIT CHANGE ALL '#SZPARM'       MYSSIDPARM
ISREDIT CHANGE ALL '#SBSDS01'      MYSSID.BSDS01
ISREDIT CHANGE ALL '#SBSDS02'      MYSSID.BSDS02
ISREDIT CHANGE ALL '#SDSNEXIT'     DSN.Vxxx.SDSNEXIT
ISREDIT CHANGE ALL '#SFECLOAD'     FEC.IBMTAPE.SFECLOAD
ISREDIT CHANGE ALL '#SCQCLOAD'     CQC.IBMTAPE.SCQCLOAD
ISREDIT CHANGE ALL '#ADHCNTRLFILE' ADH.V0A00.CONTROL
ISREDIT CHANGE ALL '#APPSRVR'      appliance.company.com
```

Parent topic: Reference information

Related tasks

- Customizing JCL members

Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

These topics document the messages and error codes issued by Security Guardium S-TAP for DB2. Messages are presented in ascending alphabetical and numerical order.

- **Error messages**
- **Error messages and codes: ADHAxxx**
- **Error messages and codes: ADHGxxx**
- **Error messages and codes: ADHIxxxx**
- **Error messages and codes: ADHKxxxx**
- **Error messages and codes: ADHPxxxx**
- **Error messages and codes: ADHQxxxx**

Parent topic: IBM Security Guardium S-TAP for Db2 on z/OS

Error messages

Security Guardium S-TAP for DB2 messages adhere to the following format: ADH*nnnx*

Where:

ADH
: Indicates that the message was issued by Security Guardium S-TAP for DB2.

nnn
: Indicates the message identification number.

x
: Indicates the severity of the message:

Table 1. Error message severity codes

Severity Code	Description
E	Indicates that an error occurred, which might or might not require operator intervention.
I	Indicates that the message is informational only.
S	Indicates that operator intervention is required before processing can continue.
W	Indicates that the message is a warning to alert you to a possible error condition.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

Error messages and codes: ADHAxxx

The following information is about error messages and codes that begin with ADHA.

- **ADHA507E**
  Callable service invocation failed with return code = *rc* and reason code = *rs*

Parent topic: Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

ADHA507E Callable service invocation failed with return code = *rc* and reason code = *rs*

Explanation

A callable service invocation failed with a return code and reason code that are identified in the message.

User response

Refer to the *IBM Db2 for z/OS®* product documentation for an explanation of this reason and return code.

Common causes of this error include:

Insufficient authorization to ADH PLAN specified in the control file
: If either of these issues are indicated by the reason code, verify that SAMPLIB member ADHGRANT was customized and submitted during configuration of the IBM® Guardium® S-TAP® for DB2® agent.

A DB2 Trace is currently running
: Issue the Db2® command -DISPLAY TRACE to view info about any audit traces that might still be running. If audit traces are running, stop them by using the Db2 command -STOP TRACE and then restart the agent. If this does not resolve the problem, check for the existence of additional messages.

If the problem is not resolved after attempting all user responses for existing additional messages, contact IBM Software Support.

Parent topic: Error messages and codes: ADHAxxx

Error messages and codes: ADHGxxx

The following information is about error messages and codes that begin with ADHG.

- **ADHG000I**
  Attempting connection to server *server-address* port=*server-port*
- **ADHG001I**
  Establishing ASC connection to server [*server-address*]
- **ADHG002I**
  Connection established to server [*server-address*]
- **ADHG003I**
  Connection re-established to [*server-address*]
- **ADHG004W**
  Connection was lost from server [*server-address*]
- **ADHG005S**
  Unable to establish a connection to a server [*server-address*]
- **ADHG006E**
  Data loss has occurred as the result of a network send failure
- **ADHG007E**
  Unable to create a communications interface
- **ADHG008S**
  Required parameter was not supplied. Parameter=*parameter-name*
- **ADHG009I**
  TCP/IP streaming disabled due to user setting.
- **ADHG010I**
  Disconnecting from server *server-name*
- **ADHG011E**
  Unable to create an output stream
- **ADHG012E**
  Unable to set socket timeout value. rc=*return-code* reason=*reason-code*
- **ADHG013I**
  Connection attempt timed out. Reattempting connection *reattempt-number* of *total-reattempts*
- **ADHG014I**
  Spillfile support enabled. Spill area size: [*size*] MB
- **ADHG015W**
  Primary server is unavailable
- **ADHG017W**
  Data is being temporarily stored in a spillfile until a connection is re-established
- **ADHG018I**
  Spillfile contents have been successfully be sent to server [*server*]
- **ADHG019S**
  Spillfile storage has been exhausted. Data loss will occur.
- **ADHG020I**
  Registering server [*server*] as eligible for failover.
- **ADHG021E**
  Spillfile is approaching [50% | 85% | 95% |100$] capacity.
- **ADHG022I**
  A connection has been established to failover server [*server*].
- **ADHG026W**
  Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.
- **ADHG027I**
  Registering server *server* as eligible for multi-stream.
- **ADHG030I**
  Security Guardium S-TAP for DB2 Collector Agent is terminating
- **ADHG031I**
  Security Guardium S-TAP for DB2 V10.1.3 [*component*] connection established
- **ADHG097E**
  Unexpected error: [*error_description*]. Return code:[*return_code*].
- **ADHG098I**
  This event will be logged due to an unexpected data condition.
- **ADHG099E**
  Unexpected error: *error-condition*
- **ADHG210I**
  A thread termination request was received for thread [*thread-token*]
- **ADHG501E**
  pbSend: Bad host name. code=*error-code*

- **ADHG502E**
  pbSend: Interface not open. code= *error-code*
- **ADHG503E**
  pbSend: Socket I/O problem. code= *error-code*
- **ADHG550E**
  Unable to send message. Connection to server is unavailable.
- **ADHG510E**
  pbWrite: No such message. code= *error-code*
- **ADHG511E**
  pbWrite: Nested too deep. code= *error-code*
- **ADHG512E**
  pbWrite: Stack underflow. code= *error-code*
- **ADHG513E**
  pbWrite: Not in message. code= *error-code*
- **ADHG514E**
  pbWrite: No such field in message. code= *error-code*
- **ADHG515E**
  pbWrite: Not a 32-bit integer field. code= *error-code*
- **ADHG516E**
  pbWrite: Not implemented. code= *error-code*
- **ADHG517E**
  pbWrite: Not a message type. code= *error-code*
- **ADHG520W**
  Encoding exception: Event exceeds protocol message size limit. code=*error-code*
- **ADHG521W**
  Total encoding exceptions encountered due to exceeded message size: *exception-count*
- **ADHG522E**
  Write failed length=*length* rc=*returncode* rsn=*reasoncode*

Parent topic: Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

ADHG000I Attempting connection to server *server-address* port=*server-port*

Explanation

The S-TAP® collector will attempt to establish a TCP/IP connection to a Guardium® system at the specified server address and port.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG001I Establishing ASC connection to server [*server-address*]

Explanation

The S-TAP® collector is preparing to establish the TCP/IP connection to the specified Guardium® system.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG002I Connection established to server [*server-address*]

Explanation

The S-TAP® collector was successful in establishing a TCP/IP connection to the Guardium® system.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG003I Connection re-established to [*server-address*]

Explanation

The S-TAP® collector was successful in re-establishing a TCP/IP connection to the Guardium® system following a disconnect.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG004W Connection was lost from server [*server-address*]

Explanation

The TCP/IP connection between the S-TAP® collector and the Guardium® system was lost. The S-TAP collector will automatically attempt to re-establish the connection, however a potential for data loss does exist if the connection is not re-established. A data loss condition is indicated by message ADHG006E.

User response

Determine the cause of the network interruption and correct the problem so that the connection can be re-established.
Parent topic: Error messages and codes: ADHGxxx

ADHG005S Unable to establish a connection to a server [*server-address*]

Explanation

The S-TAP® collector was unable to establish a TCP/IP connection to the Guardium® system.

User response

- Ensure that the Guardium system is listening for a connection at the server and port specified in message ADHG001I.
- Ensure that no firewalls are blocking connections between the collector and Guardium system.
- If port 16023 is used, ensure that AT-TLS has been configured properly between the z/OS® LPAR and the appliance.

Parent topic: Error messages and codes: ADHGxxx

ADHG006E Data loss has occurred as the result of a network send failure

Explanation

During a disconnected state, the S-TAP® collector exceeded the number of events to retain in memory while waiting for the network connection to the Guardium® system to be reestablished.

User response

- Determine the cause of the network interruption and correct the problem so that the connection can be reestablished.
- If deemed necessary, increase the SEND_FAIL_EVENT_COUNT value in the ASC ADHPARMS parameter file to increase the number of events that can be retained in memory during short outages.

Parent topic: Error messages and codes: ADHGxxx

ADHG007E Unable to create a communications interface

Explanation

An attempt to create an internal communications interface failed.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG008S Required parameter was not supplied. Parameter=*parameter-name*

Explanation

A required parameter was not supplied.

User response

Supply a parameter and value for the specified parameter.
Parent topic: Error messages and codes: ADHGxxx

ADHG009I TCP/IP streaming disabled due to user setting.

Explanation

A debug setting was specified that has disabled TCP/IP streaming between the S-TAP® collector and the Guardium® appliance.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG010I Disconnecting from server *server-name*

Explanation

The S-TAP® collector is disconnecting from the Guardium® system.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG011E Unable to create an output stream

Explanation

An attempt to create an internal output stream failed.

User response

Contact IBM® Customer Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG012E Unable to set socket timeout value. rc=*return-code* reason=*reason-code*

Explanation

An attempt to set the timeout threshold in the socket interface failed.

User response

Contact IBM® Customer Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG013I Connection attempt timed out. Reattempting connection *reattempt-number* of *total-reattempts*

Explanation

The S-TAP® collector agent was unable to establish a TCP/IP connection to the Guardium® system within the timeout period. The connection will be reattempted until the *reattempt-number* specified meets the *total-reattempts* number specified.

User response

- Ensure that the Guardium system is listening for a connection at the server and port specified in message ADHG001I.
- Ensure that there no firewalls are blocking connections between the collector and Guardium system.

Parent topic: Error messages and codes: ADHGxxx

ADHG014I Spillfile support enabled. Spill area size: [*size*] MB

Explanation

A spillfile area was successfully allocated at the specified size.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG015W Primary server is unavailable

Explanation

A connection to the primary Guardium® system is not available. Failover systems will be attempted for connection.

User response

Determine the cause of the connection interruption to the primary Guardium system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHGxxx

ADHG017W Data is being temporarily stored in a spillfile until a connection is re-established

Explanation

A Guardium® system connection is unavailable. Collected data is written to the spillfile area until a system connection can be established.

User response

Determine the cause of the system connection outage and attempt to restore the connection.
Parent topic: Error messages and codes: ADHGxxx

ADHG018I Spillfile contents have been successfully be sent to server [*server*]

Explanation

The Guardium® system connection has been restored. The spillfile data that was collected during a connection outage has been sent to the specified system.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG019S Spillfile storage has been exhausted. Data loss will occur.

Explanation

A Guardium® system connection is unavailable and the spillfile is out of space. Data collected after this time will be lost.

User response

Determine the cause of the connection outage to the system and attempt to restore the connection. Notify others of the outage as necessary.
Parent topic: Error messages and codes: ADHGxxx

ADHG020I Registering server [*server*] as eligible for failover.

Explanation

The specified server will be added to the list of failover servers to register for the connection. Registration is attempted after all failover servers have been added. A successful failover registration is indicated by message ADHG012I.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG021E Spillfile is approaching [50% | 85% | 95% |100$] capacity.

Explanation

A Guardium® system connection is unavailable and the spillfile area is at the specified capacity.

User response

Determine the cause of the connection outage to the system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHGxxx

ADHG022I A connection has been established to failover server [*server*].

Explanation

A connection to the primary Guardium® system is not available. A connection has successfully been established to one of the specified failover server.

User response

Determine the cause of the connection interruption to the primary system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHGxxx

ADHG026W Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.

Explanation

The APPLIANCE_PORT parameter currently supports a setting of 16022, but the parameter has been retained for future support. If APPLIANCE_PORT is specified with a value other than 16022, message ADHG026W is issued, and port 16022 will be used instead.

User response

Change APPLIANCE_PORT parameter setting to 16022 or remove the parameter entirely.
Parent topic: Error messages and codes: ADHGxxx

ADHG027I Registering server *server* as eligible for multi-stream.

Explanation

The specified server will be added to the list of servers that are eligible for multistream support.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG030I Security Guardium® S-TAP® for DB2® Collector Agent is terminating

Explanation

The collector is terminating.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG031I Security Guardium® S-TAP® for DB2® V10.1.3 [*component*] connection established

Explanation

The specified component successfully established a TCP/IP connection to the Guardium system.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG097E Unexpected error: [*error_description*]. Return code:[*return_code*].

Explanation

An unexpected error was encountered.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG098I This event will be logged due to an unexpected data condition.

Explanation

A collected event contained unexpected or invalid data fields. The event fields are written to DD:ADHLOG for use in diagnosing the problem.

User response

Contact IBM® Software Support with the error log.
Parent topic: Error messages and codes: ADHGxxx

ADHG099E Unexpected error: *error-condition*

Explanation

An unexpected error was encountered.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG210I A thread termination request was received for thread [*thread-token*]

Explanation

A –CANCEL THREAD command was issued by Security Guardium® S-TAP® for DB2® as a result of a request received by the Guardium system. The command ended successfully. *Thread-token* represents the cancelled thread token, as would be reported by a –DISPLAY THREAD DB2 command.

User response

No action is required.
Parent topic: Error messages and codes: ADHGxxx

ADHG501E pbSend: Bad host name. code=*error-code*

Explanation

While sending a message, the socket interface encountered a bad host name condition.

User response

- Verify that the host name value provided for APPLIANCE_SERVER in the ASC ADHPARMS parameter file is valid.
- Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHGxxx

ADHG502E pbSend: Interface not open. code= *error-code*

Explanation

While sending a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG503E pbSend: Socket I/O problem. code= *error-code*

Explanation

While sending a message, the socket interface encountered a socket I/O problem.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG550E Unable to send message. Connection to server is unavailable.

Explanation

An attempt to send a status (non-audit) message to the Guardium® system failed because a connection was unavailable.

User response

Determine the cause of the connection outage to the system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHGxxx

ADHG510E pbWrite: No such message. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG511E pbWrite: Nested too deep. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG512E pbWrite: Stack underflow. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG513E pbWrite: Not in message. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG514E pbWrite: No such field in message. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG515E pbWrite: Not a 32-bit integer field. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG516E pbWrite: Not implemented. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG517E pbWrite: Not a message type. code= *error-code*

Explanation

While building a message, a problem was encountered with an internal interface.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHGxxx

ADHG520W Encoding exception: Event exceeds protocol message size limit. code=*error-code*

Explanation

The network protocol used to communicate to the Guardium® system is limited to 64 KB in payload size. If an audited event results in a payload that exceeds this limit, this message is issued, and a truncated message is built and sent to the system. This message is only issued once per collector instance. At termination, message ADHG521W reports the total number of events impacted by this exception. The specified *error-code* value is for use by technical support.

User response

No action is required. If an excessive number of exceptions are observed, or if you are concerned that the exceptions are impacting audit data integrity, use APPLIANCE_PORT(16022), which uses a communications protocol capable of delivering events with larger payloads.
Parent topic: Error messages and codes: ADHGxxx

ADHG521W Total encoding exceptions encountered due to exceeded message size: *exception-count*

Explanation

The network protocol used to communicate to the Guardium® system is limited to 64 KB in payload size. If an audited event results in a payload that exceeds this limit, message ADHG520W is issued. At termination, this message reports the total number of events that have been impacted by this exception, displayed as *exception-count*.

User response

No action is required. If an excessive number of exceptions are observed, or if you are concerned that the exceptions are impacting audit data integrity, use APPLIANCE_PORT(16022), which uses a communications protocol capable of delivering events with larger payloads.
Parent topic: Error messages and codes: ADHGxxx

ADHG522E Write failed length=*length* rc=*returncode* rsn=*reasoncode*

Explanation

During an attempted TCP/IP data send of the length specified, the send failed with the specified return and reason code.

User response

Refer to the IBM manual, *z/OS UNIX System Services Messages and Codes*, for an explanation of the reason code. The last 4 digits of the reason code correspond to the errors of the send API. Also, review the ADHLOG of the S-TAP Collector Agent for other messages that might indicate problems with the connection between the S-TAP Collector Agent and the Guardium appliance.

This send failure might be the result of excessive amounts of data being sent to the appliance. Refer to the appliance reporting to determine whether excessive numbers of events were sent to the appliance prior to the send failure. If you determine the failure to be the result of excessive amounts of data, review and modify the active policy to decrease the amount of data that is sent to the appliance.

Parent topic: Error messages and codes: ADHGxxx

Error messages and codes: ADHIxxxx

The following information is about error messages and codes that begin with ADHI.

- **ADHI026W**
  Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.
- **ADHI031I**
  Security Guardium S-TAP for DB2 V10.1.3 [component] connection established
- **ADHI530E**
  DB2 connection failed [*function*] SQLCODE=[*sqlcode*] RSN=[*reason-code*]
- **ADHI531W**
  Option STAP_UTILITY_TS_TO_TABLE(Y) is ignored due to a previous error

- **ADHI612E**
  Termination requested as the result of a previous error
- **ADHI613E**
  SQLCODE -805 encountered for plan name [*plan_name*]
- **ADHI697E**
  Unexpected error: [*error_description*]. Return code:[*return_code*]
- **ADHI699E**
  Unexpected error: [*error-condition*]

Parent topic: Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

ADHI026W Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.

Explanation

The APPLIANCE_PORT parameter currently supports a setting of 16022, but the parameter has been retained for future support. If APPLIANCE_PORT is specified with a value other than 16022, message ADHG026W is issued, and port 16022 will be used instead.

User response

Change APPLIANCE_PORT parameter setting to 16022 or remove the parameter entirely.
Parent topic: Error messages and codes: ADHIxxxx

ADHI031I Security Guardium® S-TAP® for DB2® V10.1.3 [component] connection established

Explanation

The specified component successfully established a TCP/IP connection to the Guardium system.

User response

None action is required.
Parent topic: Error messages and codes: ADHIxxxx

ADHI530E DB2® connection failed [*function*] SQLCODE=[*sqlcode*] RSN=[*reason-code*]

Explanation

A DB2 attachment facility error occurred.

User response

An error occurred while performing a DB2 attachment function. See the *IBM® DB2 for z/OS® Messages and Codes* manual for more information about the return and reason codes.
Parent topic: Error messages and codes: ADHIxxxx

ADHI531W Option STAP_UTILITY_TS_TO_TABLE(Y) is ignored due to a previous error

Explanation

The option STAP_UTILITY_TS_TO_TABLE was set to enable collection of expanded utility information. However, an error occurred when attempting to establish the DB2® connection, which is required for this feature. The option is disabled.

User response

Review ADHLOG for occurrences of message ADHG503E to determine the cause of the DB2 connection failure.
Parent topic: Error messages and codes: ADHIxxxx

ADHI612E Termination requested as the result of a previous error

Explanation

An unrecoverable error condition was encountered. A shutdown request will sent to the collector agent.

User response

Check the ADHLOG for prior errors and attempt to resolve any previous errors.
Parent topic: Error messages and codes: ADHIxxxx

ADHI613E SQLCODE -805 encountered for plan name [*plan_name*]

Explanation

A DB2® bind error -805 was encountered for the specified plan name.

User response

Run the ADHBIND job located in the SADHSAMP library.
Parent topic: Error messages and codes: ADHIxxxx

ADHI697E Unexpected error: [*error_description*]. Return code:[*return_code*]

Explanation

An unexpected error was encountered.

User response

Contact IBM® Support.
Parent topic: Error messages and codes: ADHIxxxx

ADHI699E Unexpected error: [*error-condition*]

Explanation

An unexpected error was encountered.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHIxxxx

Error messages and codes: ADHKxxxx

The following information is about error messages and codes that begin with ADHK.

- **ADHK001I**
  Scope expression received, len = *length of expression text*
- **ADHK002I**
  Starting Compilation...
- **ADHK004I**
  Constant Pool for routine: (at *memoryLocation*).
- **ADHK005W**
  Level *level* '*compilerMessage*'.
- **ADHK101I**
  Compiling filter. Flags1 *Flags*; Compile Trace *True/False*; Runtime Trace *RuntimeTraceFlag*; RuntimeTrace *RuntimeTraceValue*; Stage 1 Requested *True/False*.
- **ADHK102I**
  Rule Expression.
- **ADHK103I**
  Profile contained no filter information for this agent.
- **ADHK104I**
  Filter Compile Failed.
- **ADHK105I**
  Variable text
- **ADHK106I**
  Compiled filter requires *bytes* bytes of dynamic save area.
- **ADHK110I**
  Rule expression:
- **ADHK111I**
  Compiling filter. flags1 *flags1* trace=*trace* runtimeTraceFlag *runtimeTraceFlag* runtimeTrace *runtimeTrace*
- **ADHK203I**
  Stage one filtering was not enabled.
- **ADHK204I**
  Error while creating stage one filter.
- **ADHK205I**
  No valid stage one filter criteria found.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

ADHK001I Scope expression received, len = *length of expression text*

Explanation

The filter compiler has received a filter expression of length *length* and expression text of *expression Text*. Only the first line of the expression text is output with this message. Only issued when trace-filter is true.

User response

None required.
Parent topic: Error messages and codes: ADHKxxxx

ADHK002I Starting Compilation...

Explanation

The expression compiler is starting to compile the filter expression. Only issued when trace-filter is true.

User response

No action is required.
Parent topic: Error messages and codes: ADHKxxxx

ADHK004I Constant Pool for routine: (at *memoryLocation*).

Explanation

This is a debugging message that shows the memory location of an important data structure for the compiled filter. This line is followed by a hexadecimal printout of the contents of that memory. Only issued when trace-filter is true.

User response

No action is required.
Parent topic: Error messages and codes: ADHKxxxx

ADHK005W Level *level* '*compilerMessage*'.

Explanation

These are messages generated by the filter compiler if there is anything wrong with the generated filter expression. The compiled filter will not be used. The agent and/or collector will shut down.

User response

Contact IBM® Software Support. Provide the agent and/or collector logs along with the xml file for the active profile at the time the message was generated.
Parent topic: Error messages and codes: ADHKxxxx

ADHK101I Compiling filter. Flags1 *Flags*; Compile Trace *True/False*; Runtime Trace *RuntimeTraceFlag*; RuntimeTrace *RuntimeTraceValue*; Stage 1 Requested *True/False*.

Explanation

An informational message is issued whenever a new profile is about to be compiled into a compiled filter.

User response

No action is required.
Parent topic: Error messages and codes: ADHKxxxx

ADHK102I Rule Expression.

Explanation

The following lines show the filter expression that was generated from the profile.

User response

No response required.
Parent topic: Error messages and codes: ADHKxxxx

ADHK103I Profile contained no filter information for this agent.

Explanation

The currently active filter had nothing specified to be collected in the current context. For example, in the ASC started task, if the filter has no targets, or if none of the targets had any events checked, then there is nothing for the ASC started task to collect.

User response

No response is required, in general. However, if you had intended data to be collected, you may wish to review the active profile. If you believe the message is issued in error, contact IBM® Software Support.
Parent topic: Error messages and codes: ADHKxxxx

ADHK104I Filter Compile Failed.

Explanation

The expression that was generated from the currently active profile could not be compiled into a filter.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHKxxxx

ADHK105I *Variable text*

Explanation

This message has been issued from the filter compiler

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHKxxxx

ADHK106I Compiled filter requires *bytes* bytes of dynamic save area.

Explanation

The compiled filter needs a certain amount of filter working memory to be able to do filtering, and this message only appears if the amount of filter working memory allocated (8192 bytes) is insufficient. This is unusual, and indicates a very large and complicated profile.

User response

You can consider reducing the size of the profile through the use of wildcards. If that is not possible, contact IBM® Software Support.
Parent topic: Error messages and codes: ADHKxxxx

ADHK110I Rule expression:

Explanation

his message will be followed by a full, multi-line, display of the filter expression generated from the profile. This message is only printed if trace-filter is true.

User response

No action is required.
Parent topic: Error messages and codes: ADHKxxxx

ADHK111I Compiling filter. flags1 *flags1* trace=*trace* runtimeTraceFlag *runtimeTraceFlag* runtimeTrace *runtimeTrace*

Explanation

An informational message issued whenever a new profile is about to be compiled into a compiled filter.

User response

No action is required.
Parent topic: Error messages and codes: ADHKxxxx

ADHK203I Stage one filtering was not enabled.

Explanation

Stage 1 filtering must be enabled.

User response

To enable stage 1 filtering, enter `STAGE1_FILTER(Y)` in the ADHCPARMS DD.
Parent topic: Error messages and codes: ADHKxxxx

ADHK204I Error while creating stage one filter.

Explanation

A bug in the filtering code prevented the correct creation of a filter for stage 1. If the stage 2 filter compiled correctly, filtering proceeds successfully at a higher overhead.

User response

Contact IBM® Software Support with XML export of the profile, and the JES output that contained this message.
Parent topic: Error messages and codes: ADHKxxxx

ADHK205I No valid stage one filter criteria found.

Explanation

Stage 1 filtering is based on a subset of the profile fields. If one or more rules in the profiles do not include at least one of the profile fields, then stage 1 filtering might not apply.

User response

Review the filtering stages section of the User's Guide and adjust the profile accordingly.
Parent topic: Error messages and codes: ADHKxxxx

Error messages and codes: ADHPxxxx

The following information is about error messages and codes that begin with ADHP.

- **ADHP000I**
  Attempting connection to server *server-address* port=*server-port*
- **ADHP001I**
  Establishing Policy connection to server [*server-address*]
- **ADHP002I**
  Connection established to server [*server-address*]
- **ADHP003I**
  Connection was re-established to [*server name*]
- **ADHP004W**
  Connection was lost from server [*server-address*]
- **ADHP005S**
  Unable to establish a connection to server [*server-address*]
- **ADHP006E**
  Data loss has occurred as the result of a network send failure
- **ADHP007E**
  Unable to create a communications interface
- **ADHP008S**
  Required parameter was not supplied. Parameter=*parameter-name*
- **ADHP009I**
  TCP/IP streaming disabled due to user setting.
- **ADHP010I**
  Disconnecting from server *server-name*
- **ADHP012I**
  Failover support enabled
- **ADHP013I**
  Connection attempt timed out. Reattempting connection *reattempt-number* of *total-reattempts*.
- **ADHP015W**
  Primary server is unavailable
- **ADHP017W**
  Data is being temporarily stored in a spillfile until a connection is re-established
- **ADHP018I**
  Spillfile contents have been successfully be sent to server [*server*]
- **ADHP019S**
  Spillfile storage has been exhausted. Dataloss will occur
- **ADHP020I**
  Registering server [*server*] as eligible for failover
- **ADHP021E**
  Spillfile is approaching [50% | 85% | 95% |100%] capacity
- **ADHP022I**
  A connection has been established to failover server [server]
- **ADHP023I**
  A persisted policy from DD:ADHPLCY is being used.

- **ADHP026W**
  Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.
- **ADHP028E**
  Required policy not available at initialization.
- **ADHP030I**
  Security Guardium S-TAP for DB2 Policy component is terminating
- **ADHP031I**
  Security Guardium S-TAP for DB2 V10.1.3 *component* connection established
- **ADHP093E**
  Policy discarded because all DB2 rules contain errors
- **ADHP094E**
  Policy discarded due to error
- **ADHP095E**
  error: rule discarded due to error
- **ADHP096E**
  rule error: *[error]*
- **ADHP097E**
  Unexpected error: [*error_description*]. Return code:[*return_code*]
- **ADHP099E**
  Unexpected error: *error-condition*
- **ADHP101W**
  Invalid value for filter. Reason: [*reason*]. Value: [*value*]
- **ADHP102E**
  Invalid value for sqlcode: [*_sqlcode_*]
- **ADHP110I**
  Security Guardium S-TAP for DB2 mode: *****
- **ADHP111I**
  STAP command [STAP MODIFY command]
- **ADHP120I**
  Installed Policy:
- **ADHP121I**
  [*policy segment*]
- **ADHP122I**
  Installed Quarantine:
- **ADHP123I**
  [*quarantine segment*]
- **ADHP124I**
  Installed Blocking:
- **ADHP125I**
  [*blocking segment*]
- **ADHP126I**
  STAP BLOCKING mode: [ENABLED|DISABLED|OPERATOR]
- **ADHP130I**
  Agent configuration:
- **ADHP131I**
  [*agent configuration segment*]
- **ADHP140I**
  Event Counts:
- **ADHP141I**
  [*event type*] [*total collected*]
- **ADHP142I**
  [*event type*] [*total collected*]
- **ADHP143I**
  [*event type*] [*total collected*]
- **ADHP144I**
  [*event type*] [*total collected*]
- **ADHP145I**
  [*event type*] [*total collected*]
- **ADHP146I**
  [*event type*] [*total collected*]
- **ADHP150I**
  Program levels:
- **ADHP151I**
  [*program level segment*]
- **ADHP160I**
  S-TAP allocation queue history:
- **ADHP161I**
  TimeStamp-------Queued----------Freed
- **ADHP162I**
  [*allocation queue segment*]
- **ADHP163I**
  S-TAP filter history:
- **ADHP164I**
  TimeStamp----Pass Stage 1-- ---Pass Stage2
- **ADHP165I**
  [*filter queue segment*]
- **ADHP166I**
  S-TAP IO history:
- **ADHP167I**
  TimeStamp--------Sent----------Bytes sent--------Write time

- **ADHP168I**
  [*filter queue segment*]
- **ADHP170I**
  Event count reported by the appliance at time: [*count*]
- **ADHP179E**
  Option [*option*] is invalid for STAP command
- **ADHP180I**
  [*policy* | *quarantine* | *blocking*] policy push detected.
- **ADHP183E**
  FORCE_LOG_LIMITED is enabled but APPLIANCE_PORT is not compatible.
- **ADHP182I**
  SUPPORT_FORCE_LOG_LIMITED is enabled.
- **ADHP183I**
  FORCE_LOG_LIMITED is not supported by the appliance.
- **ADHP184I**
  A pushed down [*policy* | *blocking* | *quarantine*] is in use.
- **ADHP185I**
  A [*policy* | *quarantine* | *blocking*] from DD is in use.
- **ADHP186I**
  A [*policy* | *quarantine* | *blocking*] from DD is in use, ignoring any pushed down policy.
- **ADHP188I**
  Blocking policy removed.
- **ADHP189W**
  There is no table found in database: [*database name*]
- **ADHP190W**
  DB2 object: [*object type*] with name: [*object name*] does not exist.
- **ADHP191W**
  Blocking is NOT ACTIVE because there is no valid target in the policy.
- **ADHP192E**
  SQL statement execution was unsuccessful, SQLCODE is: [*sqlcode value*] SQLSTATE is: [*sqlstate value*]
- **ADHP193I**
  STAP Logging command pushed down from UI to request STAP logging information.
- **ADHP200E**
  Unexpected element in policy definition: *<element>*
- **ADHP201E**
  A policy must contain at least one rule
- **ADHP203E**
  Duplicate schema specification: [*schema-name*]
- **ADHP204E**
  Duplicate table specification: [*table-name*]
- **ADHP205E**
  Duplicate First Read event specification.
- **ADHP206E**
  Duplicate First Change event specification.
- **ADHP207E**
  Expected <*policy*> specification but found <*****>.
- **ADHP208E**
  Policy syntax error
- **ADHP209E**
  Error in opening data set: [*dataset*]
- **ADHP210I**
  A thread termination request was received for thread [*thread ID*]
- **ADHP211W**
  Policy syntax error [*error*]
- **ADHP212W**
  [*policy* | *quarantine* | *blocking*] not enabled for ddname [*ddname*] reason: XML error
- **ADHP213E**
  Blocking policy syntax error: Invalid network [*network*]
- **ADHP214E**
  Blocking policy syntax error: Invalid netmask [*netmask*]
- **ADHP215E**
  Blocking policy syntax error: Invalid IP address [*IP address*]
- **ADHP216W**
  Blocking policy is ignored due to a previous error.
- **ADHP217W**
  Incomplete rule discarded. Rule name: [*_rule-name_*]
- **ADHP218W**
  Only one SQLCODE list is allowed. SQLCODE is discarded: [*sqlcode*]
- **ADHP220I**
  Appliance connect retry count has been reached, appliance ping rate is now increased to [*number*]
- **ADHP250E**
  Unable to send message. Connection to server is unavailable.
- **ADHP550E**
  Unable to send message. Connection to server is unavailable

Parent topic: Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

ADHP000I Attempting connection to server *server-address* port=*server-port*

Explanation

The S-TAP® policy component will attempt to establish a TCP/IP connection to a Guardium® system at the specified server address and port.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP001I Establishing Policy connection to server [*server-address*]

Explanation

The Security Guardium® S-TAP® for DB2® policy component is preparing to establish the TCP/IP connection to the specified Guardium system.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP002I Connection established to server [*server-address*]

Explanation

The S-TAP® policy component was successful in establishing a TCP/IP connection to the Guardium® system.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP003I Connection was re-established to [*server name*]

Explanation

The S-TAP® policy component was successful in establishing a TCP/IP connection to the Guardium® system following a disconnect.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP004W Connection was lost from server [*server-address*]

Explanation

The TCP/IP connection between the S-TAP® policy component and the Guardium® system was lost. The S-TAP policy component will automatically attempt to reestablish the connection, however a potential for data loss exists if the connection is not established. A data loss condition is indicated by message ADHP006E.

User response

Determine the cause of the network interruption and correct the problem so that the connection can be established.
Parent topic: Error messages and codes: ADHPxxxx

ADHP005S Unable to establish a connection to server [*server-address*]

Explanation

The S-TAP® Policy component was unable to establish a TCP/IP connection to the Guardium® system.

User response

- Ensure that the Guardium system is listening for a connection at the server and port specified in message ADHP001I. .
- Ensure that there are no firewalls blocking connections between the collector and the Guardium system.

Parent topic: Error messages and codes: ADHPxxxx

ADHP006E Data loss has occurred as the result of a network send failure

Explanation

During a disconnection, the S-TAP® policy component exceeded the number of events that can be retained in memory while waiting for the network connection to the Guardium® system to be reestablished.

User response

- Determine the cause of the network interruption and correct the problem so that the connection can be established.
- If necessary, increase the SEND_FAIL_EVENT_COUNT value in the ASC ADHPARMS parameter file to increase the number of events that can be retained in memory during short outages.

Parent topic: Error messages and codes: ADHPxxxx

ADHP007E Unable to create a communications interface

Explanation

An attempt to create an internal communications interface failed.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHPxxxx

ADHP008S Required parameter was not supplied. Parameter=*parameter-name*

Explanation

A required parameter was not supplied.

User response

Supply a parameter and value for the specified parameter.
Parent topic: Error messages and codes: ADHPxxxx

ADHP009I TCP/IP streaming disabled due to user setting.

Explanation

A debug setting was specified that has disabled TCP/IP streaming between the S-TAP® policy component and the Guardium® system.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP010I Disconnecting from server *server-name*

Explanation

The S-TAP® policy component is disconnecting from the Guardium® system.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP012I Failover support enabled

Explanation

One or more failover servers were successfully registered with the communications interface, enabling failover support.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP013I Connection attempt timed out. Reattempting connection *reattempt-number* of *total-reattempts.*

Explanation

The S-TAP® policy component was unable to establish a TCP/IP connection to the Guardium® system within the timeout period. An attempt to be made to reestablish the connection until the *reattempt-number* reaches the *total-reattempts* number.

User response

- Ensure that the Guardium system is listening for a connection at the server and port specified in message ADHP001I.
- Ensure that no firewalls are blocking connections between the collector and Guardium system.

Parent topic: Error messages and codes: ADHPxxxx

ADHP015W Primary server is unavailable

Explanation

A connection to the primary Guardium® system is not available. Failover appliances will be attempted for connection.

User response

Determine the cause of the connection interruption to the primary system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHPxxxx

ADHP017W Data is being temporarily stored in a spillfile until a connection is re-established

Explanation

A Guardium® system connection is unavailable and collected data is being written to the spillfile area until an system connection can be restored.

User response

Determine the cause of the connection outage to the system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHPxxxx

ADHP018I Spillfile contents have been successfully be sent to server [*server*]

Explanation

The spillfile data that was collected during a connection outage has been sent to the specified Guardium® system upon reconnection.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP019S Spillfile storage has been exhausted. Dataloss will occur

Explanation

A Guardium® system connection is unavailable and the spillfile is out of space. Data collected after this time will be lost.

User response

Determine the cause of the connection outage to the system and attempt to restore the connection. Notify others of the outage as necessary.
Parent topic: Error messages and codes: ADHPxxxx

ADHP020I Registering server [*server*] as eligible for failover

Explanation

The specified server will be added to the list of failover servers to register for the connection. Registration is attempted after all failover servers have been added. A successful failover registration is indicated by message ADHP012I.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP021E Spillfile is approaching [50% | 85% | 95% |100%] capacity

Explanation

A Guardium® system connection is unavailable and the spillfile area has reached the specified percentage of capacity.

User response

Determine the cause of the connection outage to the system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHPxxxx

ADHP022I A connection has been established to failover server [server]

Explanation

A connection to the primary Guardium® system is not available. A connection has successfully been established to one of the specified failover server.

User response

Determine the cause of the connection interruption to the primary system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHPxxxx

ADHP023I A persisted policy from DD:ADHPLCY is being used.

Explanation

The S-TAP® policy component was unable to establish a connection to the Guardium® system. A persisted policy from DD:ADHPLCY is being used.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP026W Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.

Explanation

The APPLIANCE_PORT parameter currently supports a setting of 16022, but the parameter has been retained for future support. If APPLIANCE_PORT is specified with a value other than 16022, message ADHG026W is issued, and port 16022 will be used instead.

User response

Change APPLIANCE_PORT parameter setting to 16022 or remove the parameter entirely.
Parent topic: Error messages and codes: ADHPxxxx

ADHP028E Required policy not available at initialization.

Explanation

At startup, the policy manager did not receive a policy from the Guardium appliance or policy DD.

User response

If APPLIANCE_SERVER_LIST is set to *FAILOVER*, this problem can be resolved by verifying that either:

- the primary server is active and a policy is installed, or
- the persistence policy DD is configured and has a valid policy installed from a previous policy.

IF APPLIANCE_SERVER_LIST is set to *MULTI_STREAM*, verify that the primary server is active during startup.
Parent topic: Error messages and codes: ADHPxxxx

ADHP030I Security Guardium® S-TAP® for DB2® Policy component is terminating

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP031I Security Guardium® S-TAP® for DB2® V10.1.3 *component* connection established

Explanation

The S-TAP Policy component successfully established a TCP/IP connection to the Guardium system.

User response

No action is required.

Parent topic: Error messages and codes: ADHPxxxx

ADHP093E Policy discarded because all DB2® rules contain errors

Explanation

All of the DB2 collection profile interception policies that were pushed down from the Guardium® appliance contain errors. As a result, Security Guardium S-TAP® for DB2 collection is deactivated.

User response

Review the ADHLOG for messages that were issued prior to this message that indicate why the DB2 rules were discarded. Examples of relevant messages include ADHP096E and ADHP101W. Use the reason and value that is reported in the message to correct the incorrect value or error in the collection policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP094E Policy discarded due to error

Explanation

One or more errors were detected while processing an interception policy that was pushed down from the Guardium appliance. As a result, the entire policy, as well as any rules that are contained within the policy, are ignored.

User response

Review the ADHLOG for messages that were issued prior to this message (for example, ADHP101W) that indicate why the policy was discarded. Use the reason and value that is reported in the message to correct the incorrect value or error in the collection policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP095E error: rule discarded due to error

Explanation

One or more errors were detected while processing an interception policy rule that was pushed down from the Guardium appliance. As a result, the rule containing these errors is ignored.

User response

Review the ADHLOG for messages that were issued prior to this message that indicate why the rule was discarded. Examples of relevant messages include ADHP096E and ADHP101W. Use the reason and value that is reported in the message to correct the incorrect value or error in the collection policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP096E rule error: *[error]*

Explanation

An error was detected while processing an interception policy rule that was pushed down from the Guardium appliance.

User response

Use the error text that is provided in this message to correct the value or error in the collection policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP097E Unexpected error: [*error_description*]. Return code:[*return_code*]

Explanation

An unexpected error was encountered.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHPxxxx

ADHP099E Unexpected error: *error-condition*

Explanation

An unexpected error was encountered.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHPxxxx

ADHP101W Invalid value for filter. Reason: [*reason*]. Value: [*value*]

Explanation

An invalid value was detected while processing the collection policy received from the Guardium® system.

User response

Attempt to correct the invalid value or error in the collection policy by referencing the reason and value reported in the message.
Parent topic: Error messages and codes: ADHPxxxx

ADHP102E Invalid value for sqlcode: [*_sqlcode_*]

Explanation

A SQL code that was detected while processing the collection policy from the IBM® Guardium® system is not valid.

User response

Attempt to correct the SQL code in the collection policy by referencing the value that is reported in the message. See *SQL error codes* in the IBM Knowledge Center for more information.
Parent topic: Error messages and codes: ADHPxxxx

ADHP110I Security Guardium® S-TAP® for DB2® mode: *****

Explanation

This message is issued when information about the event streaming mode is requested by issuing the /F STAP command, where ***** is either *STREAMING EVENTS* or *POLICY SIMULATION*.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP111I STAP command [STAP MODIFY command]

Explanation

This message indicates that an S-TAP MODIFY command has been issued.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP120I Installed Policy:

Explanation

The header of the installed policy

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP121I [*policy segment*]

Explanation

A segment of the installed policy

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP122I Installed Quarantine:

Explanation

The header of the installed quarantine policy

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP123I [*quarantine segment*]

Explanation

A segment of the installed quarantine policy

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP124I Installed Blocking:

Explanation

The header of the installed blocking policy

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP125I [*blocking segment*]

Explanation

A segment of the installed blocking policy

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP126I STAP BLOCKING mode: [ENABLED|DISABLED|OPERATOR]

Explanation

This message indicates whether S-TAP blocking is enabled, disabled, or in operator mode.

User response

No action is required. See SQL Blocking for more information.
Parent topic: Error messages and codes: ADHPxxxx

ADHP130I Agent configuration:

Explanation

The header of the agent configuration

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP131I [*agent configuration segment*]

Explanation

A segment of the agent configuration

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP140I Event Counts:

Explanation

The header of the event collection statistics

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP141I [*event type*] [*total collected*]

Explanation

The total count collected for the event

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP142I [*event type*] [*total collected*]

Explanation

The total count collected for the event

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP143I [*event type*] [*total collected*]

Explanation

The total count collected for the event

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP144I [*event type*] [*total collected*]

Explanation

The total count collected for the event

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP145I [*event type*] [*total collected*]

Explanation

The total count collected for the event

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP146I [*event type*] [*total collected*]

Explanation

The total count collected for the event

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP150I Program levels:

Explanation

The header of S-TAP program levels

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP151I [*program level segment*]

Explanation

A segment of S-TAP program levels

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP160I S-TAP allocation queue history:

Explanation

The header of S-TAP allocation queue history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP161I *TimeStamp-------Queued-----------Freed*

Explanation

The subheader of S-TAP allocation queue history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP162I [*allocation queue segment*]

Explanation

A segment of the allocation queue history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP163I S-TAP filter history:

Explanation

The header of S-TAP filter history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP164I *TimeStamp----Pass Stage 1-- ---Pass Stage2*

Explanation

The subheader of the S-TAP filter history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP165I [*filter queue segment*]

Explanation

A segment of S-TAP filter history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP166I S-TAP IO history:

Explanation

The header of S-TAP IO history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP167I *TimeStamp--------Sent----------Bytes sent--------Write time*

Explanation

The subheader of S-TAP IO history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP168I [*filter queue segment*]

Explanation

A segment of S-TAP IO history

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP170I Event count reported by the appliance at time: [*count*]

Explanation

Number of collected events reported by the appliance.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP179E Option [*option*] is invalid for STAP command

Explanation

An invalid value was detected while processing the S-TAP command.

User response

Check the command and try again.
Parent topic: Error messages and codes: ADHPxxxx

ADHP180I [*policy* | *quarantine* | *blocking*] policy push detected.

Explanation

A policy pushdown from the Guardium appliance has been detected.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP183E FORCE_LOG_LIMITED is enabled but APPLIANCE_PORT is not compatible.

Explanation

The FORCE_LOG_LIMITED parameter is enabled but APPLIANCE_PORT is not set correctly.

User response

Check the compatible values for FORCE_LOG_LIMITED and APPLIANCE_PORT.
Parent topic: Error messages and codes: ADHPxxxx

ADHP182I SUPPORT_FORCE_LOG_LIMITED is enabled.

Explanation

The S-TAP has been configured not to collect host variables.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP183I FORCE_LOG_LIMITED is not supported by the appliance.

Explanation

The appliance does not support the FORCE_LOG_LIMITED feature.

User response

Check for the compatible appliance with which to use the FORCE_LOG_LIMITED feature.
Parent topic: Error messages and codes: ADHPxxxx

ADHP184I A pushed down [*policy* | *blocking* | *quarantine*] is in use.

Explanation

Policy push down is in use.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP185I A [*policy* | *quarantine* | *blocking*] from DD is in use.

Explanation

A policy supplied by DD is in use rather than one from push down.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP186I A [*policy* | *quarantine* | *blocking*] from DD is in use, ignoring any pushed down policy.

Explanation

A policy supplied by DD is in use. Any pushed down policy will be discarded.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP188I Blocking policy removed.

Explanation

All blocking policies have been uninstalled.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP189W There is no table found in database: [*database name*]

Explanation

The database [*database name*] that was specified in the blocking policy is either empty or not defined.

User response

Rebuild the blocking policy with a valid database for blocking to be active for the database.
Parent topic: Error messages and codes: ADHPxxxx

ADHP190W DB2 object: [*object type*] with name: [*object name*] does not exist.

Explanation

The DB2 object [*object type*] specified in the blocking policy does not exist.

User response

Rebuild the blocking policy with valid blocking targets for blocking to be active for the DB2 object.
Parent topic: Error messages and codes: ADHPxxxx

ADHP191W Blocking is NOT ACTIVE because there is no valid target in the policy.

Explanation

No valid blocking target has been found in the blocking policy. Blocking will not be activated.

User response

Rebuild the blocking policy with valid blocking targets for blocking to be activated.
Parent topic: Error messages and codes: ADHPxxxx

ADHP192E SQL statement execution was unsuccessful, SQLCODE is: [*sqlcode value*] SQLSTATE is: [*sqlstate value*]

Explanation

A SQL statement execution was unsuccessful during policy pushdown process.

User response

Determine the cause of the SQLCODE. Correct the installed policy if necessary.
Parent topic: Error messages and codes: ADHPxxxx

ADHP193I STAP Logging command pushed down from UI to request STAP logging information.

Explanation

S-TAP logging levels provide log information as follows:

Level 0
: Logs program levels, event queue statistics, agent configuration, policy, and event counts.

Level 1
: Logs agent configuration, policy, and event counts.

Level 2
: Logs agent configuration.

Level 3
: Logs policy.

Level 4 or higher
: Logs event counts.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP200E Unexpected element in policy definition: *<element>*

Explanation

An unexpected element has been found while parsing policy.

User response

Correct the unexpected element and update the policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP201E A policy must contain at least one rule

Explanation

No rule was found in the policy.

User response

Update the policy to contains at least one rule.
Parent topic: Error messages and codes: ADHPxxxx

ADHP203E Duplicate schema specification: [*schema-name*]

Explanation

A duplicated schema within one target has been detected.

User response

Update the policy with only one schema per target.
Parent topic: Error messages and codes: ADHPxxxx

ADHP204E Duplicate table specification: [*table-name*]

Explanation

A duplicate table within one target has been detected.

User response

Update the policy with only one table per target.
Parent topic: Error messages and codes: ADHPxxxx

ADHP205E Duplicate First Read event specification.

Explanation

A duplicate First Read event has been detected.

User response

Update the policy with only one First Read event per target.
Parent topic: Error messages and codes: ADHPxxxx

ADHP206E Duplicate First Change event specification.

Explanation

A duplicate First Change event has been detected.

User response

Update the policy with only one First Change event per target.
Parent topic: Error messages and codes: ADHPxxxx

ADHP207E Expected <*policy*> specification but found <***>.

Explanation

The <*policy*> tag was expected but a different tag (<***>) was found.

User response

Correct the policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP208E Policy syntax error

Explanation

A syntax error was found while parsing the policy.

User response

Correct the policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP209E Error in opening data set: [*dataset*]

Explanation

An error occurred while opening a data set for policy parsing.

User response

Make sure the dataset exists and is associated with the appropriate permissions.
Parent topic: Error messages and codes: ADHPxxxx

ADHP210I A thread termination request was received for thread [*thread ID*]

Explanation

A termination request was received for thread [*thread ID*].

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP211W Policy syntax error [*error*]

Explanation

A syntax error was found while parsing the policy.

User response

Correct the policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP212W [*policy* | *quarantine* | *blocking*] not enabled for ddname [*ddname*] reason: XML error

Explanation

The policy from DD is not enabled because a syntax error was found.

User response

Correct the policy in the DD.
Parent topic: Error messages and codes: ADHPxxxx

ADHP213E Blocking policy syntax error: Invalid network [*network*]

Explanation

Network value is not valid in the installed blocking policy.

User response

Correct the network value and reinstall the blocking policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP214E Blocking policy syntax error: Invalid netmask [*netmask*]

Explanation

Netmask value is not valid in the installed blocking policy.

User response

Correct the netmask value and reinstall the blocking policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP215E Blocking policy syntax error: Invalid IP address [*IP address*]

Explanation

IP address value is not valid in the blocking policy.

User response

Correct the IP address value and reinstall the blocking policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP216W Blocking policy is ignored due to a previous error.

Explanation

The installed blocking policy contains a syntax error. The blocking policy is discarded.

User response

Resolve the error and reinstall the blocking policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP217W Incomplete rule discarded. Rule name: [_*rule-name*_]

Explanation

An incomplete policy rule is detected.

System action

The rule is discarded.

User response

Use the Guardium Policy Builder of the Guardium® appliance interface to define and manage data collection and filtering. Correct the specified rule *rule-name* and add the necessary filters to make it a complete rule.
Parent topic: Error messages and codes: ADHPxxxx

ADHP218W Only one SQLCODE list is allowed. SQLCODE is discarded: [*sqlcode*]

Explanation

More than one SQLCODE list is detected.

System action

The first list is accepted. Additional lists are discarded.

User response

Ensure that there is only one SQLCODE list for each installed policy.
Parent topic: Error messages and codes: ADHPxxxx

ADHP220I Appliance connect retry count has been reached, appliance ping rate is now increased to [*number*]

Explanation

Ping rate has been increased to a larger value after reaching the specified number of APPLIANCE_CONNECT_RETRY_COUNT attempts.

User response

No action is required.
Parent topic: Error messages and codes: ADHPxxxx

ADHP250E Unable to send message. Connection to server is unavailable.

Explanation

S-TAP was unable to send messages to the appliance.

User response

Make sure the appliance is online and reachable by the S-TAP.
Parent topic: Error messages and codes: ADHPxxxx

ADHP550E Unable to send message. Connection to server is unavailable

Explanation

An attempt to send a non-audit status message to the Guardium® system failed because no connection to the appliance is available.

User response

Determine the cause of the connection outage to the system and attempt to restore the connection.
Parent topic: Error messages and codes: ADHPxxxx

Error messages and codes: ADHQxxxx

The following information is about error messages and codes that begin with ADHQ. These messages are generated from the collector agent.

- **ADHQ1000E**
  NOT APF AUTHORIZED
- **ADHQ1001I**
  DB2 QUERY COMMON COLLECTOR INITIALIZATION IN PROGRESS FOR SUBSYSTEM
- **ADHQ1002I**
  DB2 AUDIT SQL COLLECTOR INITIALIZATION COMPLETE FOR SUBSYSTEM
- **ADHQ1003E**
  SUBSYSTEM *ssid* ALREADY ACTIVE
- **ADHQ1004I**
  QUERY COMMOON COLLECTOR TERMINATION IN PROGRESS FOR SUBSYSTEM *subsystem*
- **ADHQ1005I**
  QUERY COMMON COLLECTOR TERMINATION COMPLETE FOR SUBSYSTEM *ssid*
- **ADHQ1006E**
  statement DD STATEMENT MISSING
- **ADHQ1007E**
  INVALID USERID SPECIFIED FOR AUTHID
- **ADHQ1010I**
  DEBUG MODE ON
- **ADHQ1011I**
  DEBUG MODE OFF
- **ADHQ1016E**
  INVALID COMMAND SYNTAX
- **ADHQ1017E**
  INVALID COMMAND
- **ADHQ1019I**
  INTERVAL EXTERNALIZATION MODE OFF
- **ADHQ1020E**
  DB2 SUBSYSTEM *ssid* IS NOT DEFINED
- **ADHQ1024E**
  dsn SPECIFICATION INVALID
- **ADHQ1026E**
  SHARED MEMORY FAILURE FOR OBJECT *object request* RC =*rc* RS=*rs*
- **ADHQ1027I**
  CPU=*CPU Type-CPU Model-CPU Manufacturer*. *OS Name OS Version.OS Release.OS Modification*.
- **ADHQ1028E**
  Component requires a 64 bit processor and z/OS® 1.5 or higher.
- **ADHQ1031E**
  Serious error in master address space *address space*.
- **ADHQ1032I**
  Recreating master address space.
- **ADHQ1033E**
  Unable to create master address space *address space*.
- **ADHQ1034I**
  Master address space has started.
- **ADHQ1035E**
  Unable to restart master (RS=rc).
- **ADHQ1055E**
  CQM1055E DB2 ssid IS EXPERIENCING STORAGE CONSTRAINTS, DATA LOSS MAY OCCUR, REASON=code
- **ADHQ1060I**
  ZIIP SUPPORT IS NOT ACTIVE. *nnnnnnnn* RC=*yy* RSN=*zzzzzzzz nnnnnnnn* is the name of the service that failed with a nonzero return code (RC).
- **ADHQ1061E**
  MISSING PARAMETER: *parameter*
- **ADHQ1062E**
  COMMUNICATION INTERFACE DISABLED BY CROSS MEMORY FAILURE
- **ADHQ1062I**
  ZIIP SUPPORT IS INSTALLED
- **ADHQ1065E**
  REQUIRED DATA ACCESS COMMON COLLECTOR MODULE NOT FOUND
- **ADHQ1066E**
  Subsystem terminating due to abend while compiling the collection profile. SVCDUMP collected.
- **ADHQ1070E**
  Terminating due to XML profile processing error RC (xxxxxxxx)
- **ADHQ1071E**
  Terminating due to missing XML profile at start up
- **ADHQ1080I**
  POLICY MANAGER STARTED.
- **ADHQ1081I**
  POLICY MANAGER STOPPED.
- **POLICY PUSH DETECTED.**
- **ADHQ1083I**
  POLICY PUSH SENT.
- **ADHQ1084I**
  QUARANTINE ONLY POLICY DETECTED.
- **ADHQ1085I**
  CURRENT QUARANTINE POLICY IS REMOVED.
- **ADHQ1086I**
  BOTH NEW POLICY AND QUARANTINE POLICY DETECTED.
- **ADHQ1086E**
  ADHQ1086E *statement* DD STATEMENT MISSING

- **ADHQ1153E**
  RETURN CODE *return_code* REASON CODE *reason_code* WAS ENCOUNTERED DURING TRANSLATION SOURCE CCSID *ccsid* TARGET CCSID *ccsid*
- **ADHQ1202I**
  STORAGE CONSTRAINT RELIEVED FOR SPACE – *space* – OCCURRENCES: *count*
- **ADHQ1203I**
  ASID=*asid*,TCB=*tcb*,CPID=*cpid*, MODULE=*module*,ADDR=*addr*, RC=*rc*,RSN=*rsn*
- **ADHQ1204I**
  FUNC=*func*,SP=*subpool*,FLG2=*flag*,FLG3=*flag*
- **ADHQ1205E**
  ISM ERROR OCCURRED, DETAIL FOLLOWS: *note*
- **ADHQ1209I**
  ISM ERROR RC=*rc*,RSN=*rsn*,SPACE – *space*
- **ADHQ1210E**
  ISM SPACE IS DISABLED – space
- **ADHQ1211I**
  AN ABEND OCCURRED DURING ISM PROCESSING FOR SPACE – *space*
- **ADHQ1212E**
  AN ERROR OCCURRED IN THE EXTENT EXIT ROUTINE FOR SPACE – *space*
- **ADHQ1213W**
  SPACE IS FULL AND NO MORE EXTENTS CAN BE OBTAINED FOR SPACE – space
- **ADHQ1214W**
  OWNER LIMIT EXCEEDED FOR SPACE – *space*
- **ADHQ1215W**
  SPACE IS FULL AND NO MORE LARGE EXTENTS CAN BE OBTAINED FOR SPACE – *space*
- **ADHQ1216E**
  EXTENT PROCESSING FAILED (ABEND) FOR SPACE – *space*
- **ADHQ1217W**
  SPACE IS FULL AND NO MORE LARGE EXTENTS CAN BE OBTAINED FOR SPACE – *space*
- **ADHQ1218W**
  MAXIMUM EXTENTS HAS BEEN REACHED FOR SPACE – *space*
- **ADHQ1219W**
  ALL ISMERROR MESSAGE BLOCKS ARE IN USE
- **ADHQ1500E**
  ABNORMAL EOT FOR *subtask* SUBTASK
- **ADHQ2001E**
  DB2 SUBSYSTEM *ssid* ALREADY MONITORED BY SUBSYSTEM *ssid*
- **ADHQ2002E**
  MONITORING AGENT INSTALLATION FAILED FOR SUBSYSTEM *ssid*
- **ADHQ2003I**
  FORCING MONITORING AGENT INSTALLATION FOR *ssid*
- **ADHQ2005I**
  MULTIPLE MONITORING AGENT INSTALLATION FOR SUBSYSTEM *ssid*
- **ADHQ2008E**
  DB2 SYSTEM *ssid* IS BEING MONITORED BY A 2.2 OR BELOW VERSION CQM SUBSYSTEM AND CANNOT BE AUDITED
- **ADHQ2009E**
  DB2 SYSTEM ssid WAS PREVIOUSLY MONITORED BY A 2.2 OR EARLIER CQM SUBSYSTEM qmid WHICH HAS NOT APPLIED APAR PK55535.
- **ADHQ2010I**
  CURRENTLY ACTIVE POLICY RESULTS IN DISABLED COLLECTION
- **ADHQ2013I**
  CURRENTLY ACTIVE POLICY RESULTS IN GRANT/REVOKE COLLECTION
- **ADHQ2014I**
  CURRENTLY ACTIVE POLICY RESULTS NO HOST VARIABLE COLLECTION.
- **ADHQ2015I**
  CURRENTLY ACTIVE POLICY RESULTS NEGATIVE SQL CODES COLLECTION.
- **ADHQ2016I**
  CURRENTLY ACTIVE POLICY RESULTS DB2 COMMANDS COLLECTION.
- **ADHQ2017I**
  CURRENTLY ACTIVE POLICY RESULTS IN DBNAMES OPTIMIZATION.
- **ADHQ2018I**
  CURRENTLY ACTIVE POLICY RESULTS IN A QUARANTINE LIST.
- **ADHQ2019I**
  CURRENTLY ACTIVE POLICY RESULTS IN DB2 UTILITIES COLLECTION
- **ADHQ2020I**
  CURRENTLY ACTIVE POLICY RESULTS IN FAILED LOGIN COLLECTION.
- **ADHQ2100E**
  UNRECOGNIZED PARAMETER
- **ADHQ2101E**
  PARAMETER ERROR DETECTED FOR *parameter*
- **ADHQ2103E**
  DUPLICATE PARAMETER DETECTED FOR *parameter*
- **ADHQ2110E**
  TERMINATING DUE TO ERRORS IN PARAMETER FILE
- **ADHQ2111E**
  ERROR READING PARAMETER DATASET - MEMBER NOT FOUND
- **ADHQ2402I**
  DATASPACE MANAGEMENT IN PROGRESS FOR *dsmgmt*
- **ADHQ2403I**
  n DATASPACE PAGES RELEASED FOR *ssid*
- **ADHQ2408E**
  INVALID REPLY. REPLY "U" TO ACCEPT OR "R" TO REJECT

- **ADHQ2601E**
  ALLOCATION FAILED FOR VSAM DATASET *dsn* RETCD=*rc* REAS=*rs*
- **ADHQ2603E**
  DEALLOCATION FAILED FOR DATASET *data_set* RETCD=*return_code* REAS=*reason_code*
- **ADHQ3001I**
  DB2 STARTUP DETECTED FOR SUBSYSTEM *ssid*
- **ADHQ3002I**
  MONITORING AGENT STARTED FOR SUBSYSTEM *ssid*
- **ADHQ3003I**
  DB2 SHUTDOWN DETECTED FOR SUBSYSTEM *ssid*
- **ADHQ3005I**
  MONITORING AGENT DEACTIVATED FOR *ssid*
- **ADHQ3006I**
  AUDITING AGENT ACTIVATED FOR *ssid*
- **ADHQ3192E**
  LEVEL STATUS DB2(ssid) message
- **ADHQ3192I**
  LEVEL STATUS DB2(ssid) message
- **ADHQ3200I**
  DISPLAY AGENTS
- **ADHQ3201I**
  DB2 SUBYSYSTEM *ssid* AGENT ADDRESS *address*
- **ADHQ3202I**
  ssid AGENT ADDRESS *address*
- **ADHQ3203I**
  ASC DIAGNOSTIC DISPLAY:
- **ADHQ3204I**
  SDA ADDRESS *address*
- **ADHQ3205I**
  ssid ADDRESS *address*
- **ADHQ3206I**
  DIAGNOSTIC DATA FOR ABEND AT PSW *psw*
- **ADHQ3207I**
  SYSTEM COMPLETION CODE *code*
- **ADHQ3208I**
  OCCURRENCES *n* DATE *date* TIME *time*
- **ADHQ3209I**
  GPR 0-3 *info*
- **ADHQ3210I**
  GPR 4-7 *info*
- **ADHQ3211I**
  GPR 8-11 *info*
- **ADHQ3212I**
  GPR 12-15 *info*
- **ADHQ3213I**
  AR 0-3 *info*
- **ADHQ3214I**
  AR 4-7 *info*
- **ADHQ3215I**
  AR 8-11 *info*
- **ADHQ3216I**
  AR 12-15 *info*
- **ADHQ3240I**
  DB2 QM DATASPACE USAGE DISPLAY:
- **ADHQ3241I**
  dataspace DATASPACE
- **ADHQ3242I**
  NODE SIZE *size*
- **ADHQ3243I**
  TOTAL NODES *n*
- **ADHQ3244I**
  AVAILABLE NODES *n*
- **ADHQ3245I**
  PERCENT UTILIZED *n*
- **ADHQ3250I**
  POSTING INTERVAL PROCESSOR
- **ADHQ3251I**
  INTERVAL PROCESSOR NOT POSTED - DB2 UNAVAILABLE
- **ADHQ3252I**
  INTERVAL PROCESSING ALREADY IN PROGRESS
- **ADHQ3308E**
  DB2 SYSTEM ssid IS MONITORED BY DB2 QUERY MONITOR ssid WHICH HAS MISMATCHED OBJ AGENT
- **ADHQ3315E**
  MASTER SUBSYSTEM DOES NOT MATCH
- **ADHQ3402I**
  ISSUING COMMAND *cmd*
- **ADHQ3551E**
  VSAM LOGIC ERROR ENCOUNTERED WHILE ACCESSING CONTROL FILE FOR DB2 *ssid*. VSAMRC='*rc*' VSAMRS=X'*rs*'
- **ADHQ3552E**
  SETUP INFORMATION MISSING FROM CONTROL FILE FOR DB2 *ssid*

- **ADHQ3553E**
  message ERROR *message*
- **ADHQ4001E**
  CONNECT TO DB2 *ssid* FAILED FOR PLAN *plan* RETURN CODE *rc* REASON CODE *rs*
- **ADHQ4003E**
  CONNECT FAILED - DB2 NOT OPERATIONAL
- **ADHQ5010I**
  MONITORING AGENT DEINSTALLATION IN PROGRESS FOR SUBSYSTEM *ssid*
- **ADHQ5011I**
  MONITORING AGENT DEINSTALLATION COMPLETE FOR SUBSYSTEM *ssid*
- **ADHQ5012I**
  REQURESTING MONITORING AGENT ACTIVATION FOR DB2 SUBSYSTEM *ssid*
- **ADHQ5013I**
  REQUESTING MONITORING AGENT DEACTIVATION FOR DB2 SUBSYSTEM *ssid*
- **ADHQ6101E**
  LOCATE FAILED FOR *dataset* R0=*code* RC=*rc*
- **ADHQ6102E**
  SCRATCH FAILED FOR *file* SCRATCH STATUS CODE=*code* RO=*ro*
- **ADHQ7001E**
  table TABLE NOT LOCATED IN DB2 CATALOG
- **ADHQ7008E**
  QUERY COMMON COLLECTOR *ssid* NOT VALID OR HAS NOT BEEN STARTED SINCE IPL
- **ADHQ7009E**
  OUT OF SPACE CONDITION DETECTED WHILE WRITING TO THE *dsn* DATASET
- **ADHQ7010E**
  MISSING "ADD" PARAMETER FOR *parameter* AT LINE *line* COLUMN *column*
- **ADHQ7011E**
  INTERNAL ERROR - UNABLE TO RESOLVE ALTERNATE COLUMN *column*
- **ADHQ7015E**
  NUMBER OF BSDS SPECIFICATIONS INVALID OR MISSING
- **ADHQ7016E**
  DUPLICATE RECORD STORE ATTEMPTED FOR DB2 SUBSYSTEM *ssid*
- **ADHQ8001E**
  ERRORS DETECTED IN *parameters* PARAMETERS:
- **ADHQ8002E**
  UNIDENTIFIED KEYWORD DETECTED AT LINE *line* COLUMN *column*
- **ADHQ8003E**
  INVALID SYNTAX SPECIFIED FOR *parameter* NEAR LINE *line* COLUMN *column*
- **ADHQ8004E**
  PARAMETER LENGTH EXCEEDED FOR *parameter* NEAR LINE *line* COLUMN *column*
- **ADHQ8005E**
  PARAMETER MISSING FOR *parameter* NEAR LINE *line* COLUMN *column*
- **ADHQ8006E**
  NON NUMERIC DATA SPECIFIED FOR *parameter* NEAR LINE *line* COLUMN *column*
- **ADHQ8007E**
  INVALID VALUE SPECIFIED FOR *parameter* NEAR LINE *line* COLUMN *column*
- **ADHQ8008E**
  value MUST BE *value* THAN *value*
- **ADHQ8009E**
  DUPLICATE PARAMETER *parameter* AT LINE *line* COLUMN *column*
- **ADHQ8010E**
  DUPLICATE SUBPARAMETER DETECTED FOR PARAMETER *parameter* AT LINE *line* COLUMN *column*
- **ADHQ8011E**
  DB2 VERSION NOT SUPPORTED
- **ADHQ8012E**
  ERROR OPENING DDNAME *ddname*
- **ADHQ8013E**
  INVALID PARAMETER LENGTH FOR *parameter*
- **ADHQ8014E**
  LOGIC ERROR: *error*
- **ADH8022I**
  adh parameter value
- **ADH9899I**
  adh modify command

Parent topic: Messages and codes for IBM Security Guardium S-TAP for DB2 on z/OS

ADHQ1000E NOT APF AUTHORIZED

Explanation

The collector agent started task or job is not APF authorized.

User response

The collector agent requires that the target load libraries be APF-authorized.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1001I DB2® QUERY COMMON COLLECTOR INITIALIZATION IN PROGRESS FOR SUBSYSTEM

Explanation

This message appears during the normal initialization process of the collector agent.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1002I DB2® AUDIT SQL COLLECTOR INITIALIZATION COMPLETE FOR SUBSYSTEM

Explanation

This message appears during the normal initialization process of the collector agent and confirms the initialization process has completed.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1003E SUBSYSTEM *ssid* ALREADY ACTIVE

Explanation

The collector agent indicated in the message is already active and can therefore cannot process another activate command.

User response

Verify that you are activating the correct system. If you are attempting to activate a subsystem that is already active, do not attempt activation.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1004I QUERY COMMOON COLLECTOR TERMINATION IN PROGRESS FOR SUBSYSTEM *subsystem*

Explanation

This message appears during normal shutdown of the Collector Agent and indicates the collector is undergoing shutdown.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1005I QUERY COMMON COLLECTOR TERMINATION COMPLETE FOR SUBSYSTEM *ssid*

Explanation

The collector agent subsystem has been terminated. This message could appear as part of normal shutdown or as a failure to connect to a subsystem.

User response

Investigate other write-to-operator (WTO) messages preceding this one to determine the reason for the termination.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1006E *statement* DD STATEMENT MISSING

Explanation

The parameter DD statement (for example, ADHCFGP DD statement) is missing from the JCL for the collector agent started task.

User response

Create the necessary DD statement and code the appropriate parameters in the data set.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1007E INVALID USERID SPECIFIED FOR AUTHID

Explanation

The user ID entered in the AUTHID parm in the ADHCFGP data set has not been defined to RACF® or an equivalent security system.

User response

Correct the user ID, or ensure the ID is defined to your security system.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1010I DEBUG MODE ON

Explanation

Debugging mode has been turned on.

User response

None required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1011I DEBUG MODE OFF

Explanation

Debugging mode has been turned off.

User response

None required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1016E INVALID COMMAND SYNTAX

Explanation

The command syntax is invalid.

User response

Correct the command.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1017E INVALID COMMAND

Explanation

An invalid MVS™ Modify command was issued.

User response

Correct the command and execute it again.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1019I INTERVAL EXTERNALIZATION MODE OFF

Explanation

The collector agent subsystem was started with externalization mode set to off.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1020E DB2® SUBSYSTEM *ssid* IS NOT DEFINED

Explanation

The DB2 subsystem indicated in the message is not defined.

User response

Verify that you have specified the correct DB2 subsystem.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1024E *dsn* SPECIFICATION INVALID

Explanation

The data set name listed in this message is not valid.

User response

Verify that you specified the correct data set name in ADHCFGP.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1026E SHARED MEMORY FAILURE FOR OBJECT *object request* RC =*rc* RS=*rs*

Explanation

A shared memory failure has occurred for the indicated object.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1027I CPU=*CPU Type-CPU Model-CPU Manufacturer. OS Name OS Version.OS Release.OS Modification.*

Explanation

This message displays information about the CPU and the operating system.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1028E Component requires a 64 bit processor and z/OS® 1.5 or higher.

Explanation

Your system does not meet the minimum system requirements.

User response

Upgrade to the minimum requirements.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1031E Serious error in master address space *address space*.

Explanation

A serious error has occurred in the master address space specified.

User response

Verify that the master address space is available.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1032I Recreating master address space.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1033E Unable to create master address space *address space*.

Explanation

DB2® Query Monitor is not able to create the master address space specified.

User response

Many issues that cause this error relate to security setup. If you encounter this message, send your console log to IBM® Software Support.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1034I Master address space has started.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1035E Unable to restart master (RS=rc).

Explanation

The master address space could not be restarted.

User response

verify the master address space is available and restart.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1055E CQM1055E DB2® ssid IS EXPERIENCING STORAGE CONSTRAINTS, DATA LOSS MAY OCCUR, REASON=code

Explanation

The DB2 subsystem indicated in the message is experiencing storage constraints.

User response

Verify that your DB2 subsystem has the needed storage allocations.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1060I ZIIP SUPPORT IS NOT ACTIVE. *nnnnnnnn* RC=*yy* RSN=*zzzzzzzz nnnnnnnn* is the name of the service that failed with a nonzero return code (RC).

Explanation

Table 1. Return code explanations

Service	Description
IWM4ECRE (WLM Enclave Create)	The return codes and reason codes are documented in *z/OS V1R10.0 MVS™ Programming Workload Management Services*.
IWM4EoCT (WLM CPU Offload Time Service)	The return codes and reason codes are not documented in any existing WLM manual. However, RC=4 typically means no ZIIP is configured on the instance of z/OS®. If you have a ZIIP processor and it is properly configured, report the RC to the vendor.
MAXWFLOAD (Enclave SRB load service)	An error occurred trying to LOAD ADHMAXWF (the enclave SRB routine that runs on the ZIIP). Make sure you have the correct STEPLIB configured.
IEAVAPE (Z/OS Allocate Pause Element)	These return codes are described in *z/OS V1R10.0 MVS Programming Assembler Services References V2*. If the ADHQ1060I has IEAVAPE has the failing service, contact the vendor for resolution.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1061E MISSING PARAMETER: *parameter*

Explanation

The specified parameter has not been defined in the sample library member ADHCFGP.

User response

Add the missing parameter to the ADHCFGP sample library member.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1062E COMMUNICATION INTERFACE DISABLED BY CROSS MEMORY FAILURE

Explanation

A cross memory failure has occurred and as a result the communication interface has been disabled.

User response

Troubleshoot the memory failure and restart the ASC.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1062I ZIIP SUPPORT IS INSTALLED

Explanation

The collector agent has detected that WLM is configured for zIIP support. This does not necessarily indicate that zIIP processors are installed or are available for zIIP offload of collector agent processing.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1065E REQUIRED DATA ACCESS COMMON COLLECTOR MODULE NOT FOUND

Explanation

The started task did not find the Data Access Common Collector (CQC) initialization module, which prevented successful startup.

User response

Verify that the Data Access Common Collector (CQC) has been installed and that the load library is included in the started task STEPLIB concatenation
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1066E Subsystem terminating due to abend while compiling the collection profile. SVCDUMP collected.

Explanation

An abend was detected when compiling the collection profile. A memory dump was collected to gather the diagnostic information.

User response

If you are unable to take corrective measures to resolve the abend, then the SVCDUMP, the collector joblog, and the details of the collection profile in use should be reported to IBM® Software Support for resolution of this error.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1070E Terminating due to XML profile processing error RC (xxxxxxxx)

Explanation

A policy is sent from the Guardium® system to the Security Guardium S-TAP® for DB2® collector agent during their initial communication. If the policy received by the collector agent is not composed of valid XML syntax, the collector terminates.

User response

Verify that the Guardium system is properly configured, using the APPLIANCE_SERVER parameter. The system should be set up to accept connections from collectors. If the problem persists, contact IBM® Software Support with the return code specified in this message.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1071E Terminating due to missing XML profile at start up

Explanation

A policy is sent from the Guardium® system to the Security Guardium S-TAP® for DB2® collector agent during their initial communication. If the policy is not received by the collector agent during the initial communication set up, then the collector terminates.

User response

Verify that the Guardium system is properly configured, using the APPLIANCE_SERVER parameter. The appliance should be set up to accept connections from collectors. If the problem persists, contact IBM® Software Support.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1080I POLICY MANAGER STARTED.

Explanation

The internal policy manager task has started.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1081I POLICY MANAGER STOPPED.

Explanation

The internal policy manager task has stopped.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

POLICY PUSH DETECTED.

Explanation

A policy was received from the appliance.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1083I POLICY PUSH SENT.

Explanation

The policy was sent to Audit SQL Collector.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1084I QUARANTINE ONLY POLICY DETECTED.

Explanation

A pushed policy was included on a quarantine list. The currently active audit policy is unchanged and is still active.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1085I CURRENT QUARANTINE POLICY IS REMOVED.

Explanation

A new policy push occurred which resulted in the removal of the quarantine list.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1086I BOTH NEW POLICY AND QUARANTINE POLICY DETECTED.

Explanation

A new policy push occurred, which resulted in new policy and quarantine lists to be activated.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1086E ADHQ1086E *statement* DD STATEMENT MISSING

Explanation

The parameter DD statement (for example, ADHPARMS DD statement) is missing from the JCL for the collector agent started task.

User response

Create the necessary DD statement and code the appropriate parameters in the data set.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ1153E RETURN CODE *return_code* REASON CODE *reason_code* WAS ENCOUNTERED DURING TRANSLATION SOURCE CCSID *ccsid* TARGET CCSID *ccsid*

Explanation

An error was encountered during the translation of the indicated CCSIDs. This may be the result of not having defined conversion paths between the CCSID of the collected SQL text and CCSID 1208 when performing a DB2® offload.

User response

To offload SQL text, verify that all necessary CCSID paths to 1208 are installed. You must define conversion paths between the CCSID of the collected SQL text and CCSID 1208.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1202I STORAGE CONSTRAINT RELIEVED FOR SPACE – *space* – OCCURRENCES: *count*

Explanation

An Integrated Storage Manager error had previously occurred due to a storage constraint for the space named in the message. The storage constraint has now been relieved. The number of storage constraint occurrences for this incident is displayed in the message.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1203I ASID=*asid*,TCB=*tcb*,CPID=*cpid*, MODULE=*module*,ADDR=*addr*, RC=*rc*,RSN=*rsn*

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager error has occurred. This message provides details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1204I FUNC=*func*,SP=*subpool*,FLG2=*flag*,FLG3=*flag*

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager error has occurred. This message provides details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1205E ISM ERROR OCCURRED, DETAIL FOLLOWS: *note*

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that have been produced to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1209I ISM ERROR RC=*rc*,RSN=*rsn*,SPACE – *space*

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that have been produced to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1210E ISM SPACE IS DISABLED – space

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that have been produced to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1211I AN ABEND OCCURRED DURING ISM PROCESSING FOR SPACE – *space*

Explanation

A Query Monitor Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any dumps that may have been produced to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1212E AN ERROR OCCURRED IN THE EXTENT EXIT ROUTINE FOR SPACE – *space*

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that might been produced to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1213W SPACE IS FULL AND NO MORE EXTENTS CAN BE OBTAINED FOR SPACE – space

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager operation has failed because no more extents can be obtained for the space named in the message. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

This may be a temporary situation due to the level of DB2 activity currently monitored by Security Guardium S-TAP for DB2. If message ADHQ1202I is also issued to indicate that the Storage Constraint has ended, then processing resumes. If this situation occurs frequently, adjust the amount of data collected by Security Guardium S-TAP for DB2, or increase the amount of available memory by using the MAXIMUM_ALLOCATIONS and SMEM_SIZE parameters.

If you need assistance with modifying these parameters, provide the text of this message and messages ADHQ1203I and ADHQ1204I to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1214W OWNER LIMIT EXCEEDED FOR SPACE – *space*

Explanation

A Security Guardium® S-TAP® for DB2® Monitor Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that might have been produced to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1215W SPACE IS FULL AND NO MORE LARGE EXTENTS CAN BE OBTAINED FOR SPACE – *space*

Explanation

A Security Guardium® S-TAP® for DB2® Monitor Integrated Storage Manager operation has failed because no more large extents can be obtained for the space named in the message. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Support to diagnose the problem.

User response

This might be a temporary situation due to the level of DB2 activity currently being monitored by Security Guardium S-TAP for DB2. If message ADHQ1202I is also issued to indicate that the Storage Constraint has ended, then processing resumes. If this situation occurs frequently, adjust the amount of data collected by Security Guardium S-TAP for DB2, or increase the amount of available memory by using the MAXIMUM_ALLOCATIONS and SMEM_SIZE parameters.

If you need assistance with modifying these parameters, provide the text of this message and messages ADHQ1203I and ADHQ1204I to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1216E EXTENT PROCESSING FAILED (ABEND) FOR SPACE – *space*

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager error has occurred. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

Provide the text of this message and messages ADHQ1203I and ADHQ1204I along with any memory dumps that have been produced to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1217W SPACE IS FULL AND NO MORE LARGE EXTENTS CAN BE OBTAINED FOR SPACE – *space*

Explanation

A Security Guardium® S-TAP® for DB2® Integrated Storage Manager operation has failed because the request would have exceeded the maximum storage allocation specified in the MAXIMUM_ALLOCATIONS parameter in ADHPARMS. At the time of the error, Security Guardium S-TAP for DB2 was attempting to allocate additional storage for the space named in the message. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

This might be a temporary situation due to the level of DB2 activity currently being monitored by Security Guardium S-TAP for DB2. If message ADHQ1202I is also issued to indicate that the Storage Constraint has ended, then processing resumes. If this situation occurs frequently, adjust the amount of data collected by Security Guardium S-TAP for DB2, or increase the amount of available memory by using the MAXIMUM_ALLOCATIONS and SMEM_SIZE parameters.

If you need assistance with modifying these parameters, provide the text of this message and messages ADHQ1203I and ADHQ1204I to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1218W MAXIMUM EXTENTS HAS BEEN REACHED FOR SPACE – *space*

Explanation

An Integrated Storage Manager operation has failed because the request would have exceeded the maximum number of extents allowed for the space named in the message. This message and messages ADHQ1203I and ADHQ1204I provide details that can be used by IBM® Software Support to diagnose the situation.

User response

This might be a temporary situation due to the level of DB2® activity currently being monitored. If message ADHQ1202I is issued later to indicate that the Storage Constraint has ended, then processing resumes normally. If this situation rarely occurs, it might not be a problem. If this situation occurs frequently, adjust the amount of data collected by Security Guardium® S-TAP® for DB2, or increase the amount of available memory by using the MAXIMUM_ALLOCATIONS and SMEM_SIZE parameters.

If you need assistance with tuning these parameters, provide the text of this message and messages ADHQ1203I and ADHQ1204I to IBM Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1219W ALL ISMERROR MESSAGE BLOCKS ARE IN USE

Explanation

An Integrated Storage Manager error has occurred. However there were no free ISMERROR message blocks available.

User response

Increase the value of the ISM_ERROR_BLOCKS parameter in the ADHPARMS file. If this parameter is already set to the maximum value and the problem persists, contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ1500E ABNORMAL EOT FOR *subtask* SUBTASK

Explanation

An abnormal end of task occurred for the subtask indicated in the message.

User response

Verify conditions surrounding the abnormal end of task and reissue the subtask.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2001E DB2® SUBSYSTEM *ssid* ALREADY MONITORED BY SUBSYSTEM *ssid*

Explanation

The indicated DB2 subsystem is already being monitored by the collector agent shown in the message.

User response

A DB2 subsystem can only be monitored by a single collector agent. To monitor the DB2 subsystem with another collector agent, first stop the monitoring of the DB2 subsystem by the collector agent (shown in the message).

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2002E MONITORING AGENT INSTALLATION FAILED FOR SUBSYSTEM *ssid*

Explanation

A monitoring agent was unable to start. Another SQL-type monitoring product might be active within the specified DB2® subsystem.

User response

Check to see if another SQL-type monitoring product is active. If so, shut down the other product and restart the S-TAP® collector. If this does not resolve the problem, contact IBM® Software Support.

If you encounter message ADHQ2002E and receive a memory dump, contact IBM Software Support and provide the memory dump for diagnostic purposes.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2003I FORCING MONITORING AGENT INSTALLATION FOR *ssid*

Explanation

The collector agent has detected that a monitoring agent is already active, but is forcing installation because `FORCE (Y)` was included.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2005I MULTIPLE MONITORING AGENT INSTALLATION FOR SUBSYSTEM *ssid*

Explanation

The collector agent has installed multiple monitoring agents for the subsystem shown in the message.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2008E DB2 SYSTEM *ssid* IS BEING MONITORED BY A 2.2 OR BELOW VERSION CQM SUBSYSTEM AND CANNOT BE AUDITED

Explanation

This message indicates an incompatibility between DB2 Query Monitor and S-TAP. InfoSphere® Guardium S-TAP for DB2 Version 9.1 will not start auditing a DB2 subsystem that is running Query Monitor at Version 3.1 or earlier.

User response

Ensure that you are running compatible versions of S-TAP and Query Monitor, or run only one product at a time.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2009E DB2® SYSTEM ssid WAS PREVIOUSLY MONITORED BY A 2.2 OR EARLIER CQM SUBSYSTEM qmid WHICH HAS NOT APPLIED APAR PK55535.

Explanation

You must apply Query Monitory V2R2 APAR PK55535.

User response

Apply the required maintenance.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2010I CURRENTLY ACTIVE POLICY RESULTS IN DISABLED COLLECTION

Explanation

The currently installed collection policy, as received from the Guardium® system, results in no ASC collection. This can be the result of:

- No policies are installed on the system.
- No DB2® Collection Profile policies are installed on the system.
- No DB2 Collection Profile policies matching the Svc. Name of the collector agent SSID are installed on the system.
- No DB2 Collection Profile policies contain Object entries that would result in ASC collection.

User response

If ASC collection is expected when this message is issued, review installed policy definitions in the Guardium system administration interface for the previously listed conditions. If no ASC collection is expected when this message is issued, no action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2013I CURRENTLY ACTIVE POLICY RESULTS IN GRANT/REVOKE COLLECTION

Explanation

The activated policy enables the collection of GRANT and REVOKE SQL statements. GRANT and REVOKE SQL statements are collected if they match the policy filter criteria.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2014I CURRENTLY ACTIVE POLICY RESULTS NO HOST VARIABLE COLLECTION.

Explanation

Host variables, which are also known as BIND variables, are not collected.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2015I CURRENTLY ACTIVE POLICY RESULTS NEGATIVE SQL CODES COLLECTION.

Explanation

The active policy contains a negative SQL code list that results in the collection of events ending with a negative SQL code.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2016I CURRENTLY ACTIVE POLICY RESULTS DB2 COMMANDS COLLECTION.

Explanation

Collection of COMMAND events is enabled.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2017I CURRENTLY ACTIVE POLICY RESULTS IN DBNAMES OPTIMIZATION.

Explanation

The currently active policy contains rules with DBNAME filters, which enables optimized filtering of audit events.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2018I CURRENTLY ACTIVE POLICY RESULTS IN A QUARANTINE LIST.

Explanation

The active policy contains a quarantine list that might cause DB2 activity to be quarantined.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2019I CURRENTLY ACTIVE POLICY RESULTS IN DB2 UTILITIES COLLECTION

Explanation

The active policy enables the collection of DB2 utilities.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2020I CURRENTLY ACTIVE POLICY RESULTS IN FAILED LOGIN COLLECTION.

Explanation

The active policy enables the collection of Failed Login events.

User response

No action is required.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ2100E UNRECOGNIZED PARAMETER

Explanation

The collector agent has encountered an unrecognized parameter.

User response

Check the startup parameters to ensure that the parameters specified are all valid.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2101E PARAMETER ERROR DETECTED FOR *parameter*

Explanation

The collector agent has encountered an error in one of the startup parameters.

Note: Message ADHQ2101E can be issued when the collector agent is started if the ADHCFGP file specifies primary space allocations for back store data sets that are less than the default.

User response

Check the startup parameters to ensure that all are specified properly. Check that primary space allocations for back store data sets are not set for less than their default values.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2103E DUPLICATE PARAMETER DETECTED FOR *parameter*

Explanation

Duplicate parameters were specified in the Query Common Collector startup parameters.

User response

Check the startup parameters to ensure that all are specified properly. Remove any duplicate parameters.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2110E TERMINATING DUE TO ERRORS IN PARAMETER FILE

Explanation

An error in the collector agent parameter file caused the termination of processing.

User response

Verify that the input you specified for your collector agent parameters in ADHCFGP is valid and correct for your objectives.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2111E ERROR READING PARAMETER DATASET - MEMBER NOT FOUND

Explanation

The collector agent encountered an error while attempting to read the ADHCFGP data set. The ADHPARMS DD statement specified a PDS data set and the member name specified did not exist.

User response

Correct the JCL specification for the ADHPARMS DD statement and specify a valid member name.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2402I DATASPACE MANAGEMENT IN PROGRESS FOR *dsmgmt*

Explanation

Indicates dataspace management is in progress for the subsystem shown in the message.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2403I *n* DATASPACE PAGES RELEASED FOR *ssid*

Explanation

Displays the number of dataspace pages that have been released for the subsystem shown in the message.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2408E INVALID REPLY. REPLY "U" TO ACCEPT OR "R" TO REJECT

Explanation

The replay you entered is not valid.

User response

Enter U to accept or R to reject.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2601E ALLOCATION FAILED FOR VSAM DATASET *dsn* RETCD=*rc* REAS=*rs*

Explanation

This message is issued by the started task if there is a problem during the dynamic allocation of a data set. When this message occurs, the collector agent stops and the startup process and terminates.

User response

To further diagnose and resolve the problem using the return code and reason code listed in the message, refer to the *MVS™ Programming Authorized Assembler Services Guide* (SA22-7608-07).

Parent topic: Error messages and codes: ADHQxxxx

ADHQ2603E DEALLOCATION FAILED FOR DATASET *data_set* RETCD=*return_code* REAS=*reason_code*

Explanation

This message reports errors encountered during the execution of a CLOSE macro instruction.

User response

To further diagnose and resolve the problem using the return code and reason code listed in the message, refer to the *z/OS® V1R1.0 DFSMS/DFP Diagnosis Reference* (GY27-7618-01) or the following Web page:

http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/BOOKS/dgt2r101/20.8.1.2
Parent topic: Error messages and codes: ADHQxxxx

ADHQ3001I DB2® STARTUP DETECTED FOR SUBSYSTEM *ssid*

Explanation

The collector agent determined that a DB2 subsystem in its monitor list has started.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3002I MONITORING AGENT STARTED FOR SUBSYSTEM *ssid*

Explanation

Security Guardium® S-TAP® for DB2® has initiated monitoring for the named subsystem.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3003I DB2® SHUTDOWN DETECTED FOR SUBSYSTEM *ssid*

Explanation

The collector agent determined that a DB2 subsystem in its monitor list has shut down.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3005I MONITORING AGENT DEACTIVATED FOR *ssid*

Explanation

The monitoring agent has been deactivated for the indicated Collector Agent.

User response

None required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3006I AUDITING AGENT ACTIVATED FOR *ssid*

Explanation

The collector agent has been instructed to start the monitoring agent for a given DB2® subsystem when it becomes active. Monitoring of SQL for the DB2 subsystem will start when the monitoring agent is started indicated by message ADHQ3002I. Monitoring will continue after message ADHQ3002I is issued until one of the following

events occur:

1. The DB2 subsystem is stopped.
2. A deactivate for the monitoring agent is performed.
3. The collector agent subsystem that is monitoring the DB2 subsystem is stopped.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3192E LEVEL STATUS DB2(ssid) message

Explanation

This message displays if a mismatch in code level exists between Security Guardium® S-TAP® for DB2® and Query Monitor. One message per mismatched code level will occur.

User response

Ensure that all the programs listed have the Query Monitor and corresponding Security Guardium S-TAP for DB2 maintenance applied.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ3192I LEVEL STATUS DB2(ssid) message

Explanation

This message displays if a mismatch in code level exists between Security Guardium® S-TAP® for DB2® and DB2 Query Monitor. This message occurs once per mismatched code level.

User response

Verify that all the programs listed have the Query Monitor and corresponding S-TAP for DB2 maintenance applied.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ3200I DISPLAY AGENTS

Explanation

This message is used in conjunction with other messages to indicate display agents.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3201I DB2® SUBYSYSTEM *ssid* AGENT ADDRESS *address*

Explanation

Indicates the DB2 subsystem and agent address.

User response

None required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3202I *ssid* AGENT ADDRESS *address*

Explanation

Indicates the monitoring agent address.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3203I ASC DIAGNOSTIC DISPLAY:

Explanation

Indicates ASC diagnostic display is in effect.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3204I SDA ADDRESS *address*

Explanation

Indicates the SDA address.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3205I *ssid* ADDRESS *address*

Explanation

This message is used in conjunction with other messages to indicate the address.

User response

None required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3206I DIAGNOSTIC DATA FOR ABEND AT PSW *psw*

Explanation

The message displays diagnostic data for the abend.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3207I SYSTEM COMPLETION CODE *code*

Explanation

The message indicates the system completion code.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3208I OCCURRENCES *n* DATE *date* TIME *time*

Explanation

Indicates the number of occurrences and the date and time at which the took place.

User response

None required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3209I GPR 0-3 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3210I GPR 4-7 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3211I GPR 8-11 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3212I GPR 12-15 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3213I AR 0-3 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3214I AR 4-7 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3215I AR 8-11 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3216I AR 12-15 *info*

Explanation

This message displays diagnostic information about the current contents of the register.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3240I DB2® QM DATASPACE USAGE DISPLAY:

Explanation

This message appears in conjunction with other messages as a result of the MVS™ Modify command DISPLAY DATASPACES.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3241I *dataspace* DATASPACE

Explanation

This message appears in conjunction with ADHQ3240I as a result of the MVS™ Modify command `DISPLAY DATASPACES`.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3242I NODE SIZE *size*

Explanation

This message appears in conjunction with ADHQ3240I as a result of the MVS™ Modify command DISPLAY DATASPACES. This message lists the node size for the named data space.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3243I TOTAL NODES *n*

Explanation

This message appears in conjunction with ADHQ3240I as a result of the MVS™ Modify command `DISPLAY DATASPACES`. This message lists the total number of nodes allowed for the named data space.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3244I AVAILABLE NODES *n*

Explanation

This message appears in conjunction with ADHQ3240I as a result of the MVS™ Modify command `DISPLAY DATASPACES`. This message lists the total number of nodes available for use by the named data space.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3245I PERCENT UTILIZED *n*

Explanation

This message appears in conjunction with ADHQ3240I as a result of the MVS™ Modify command `DISPLAY DATASPACES`. This message lists the percentage of nodes used for the named data space.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3250I POSTING INTERVAL PROCESSOR

Explanation

This message appears to inform you that the interval processor has been started through an MVS™ Modify INTERVAL command.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3251I INTERVAL PROCESSOR NOT POSTED - DB2® UNAVAILABLE

Explanation

The interval processor was not started because a DB2 subsystem is not available.

User response

Verify the status of all monitored DB2 subsystems.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3252I INTERVAL PROCESSING ALREADY IN PROGRESS

Explanation

This message appears to inform you that the interval processor was already started through an MVS™ Modify `INTERVAL` command.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3308E DB2® SYSTEM ssid IS MONITORED BY DB2 QUERY MONITOR ssid WHICH HAS MISMATCHED OBJ AGENT

Explanation

This message indicates that the maintenance levels of one or more object modules do not match between the Security Guardium® S-TAP® for DB2 and Query Monitor installations. The maintenance code levels for Security Guardium S-TAP for DB2 and Query Monitor installations must match.

User response

Ensure that the maintenance levels match between the Security Guardium S-TAP for DB2 and Query Monitor installations. Apply maintenance as required to one or both environments to ensure that the maintenance levels match.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3315E MASTER SUBSYSTEM DOES NOT MATCH

Explanation

For monitoring and auditing to be active on the DB2® subsystem, a DB2 subsystem that is monitored by DB2 Query Monitor or Workload Replay for DB2 for z/OS® or audited by Security Guardium® S-TAP® for DB2 must have a matching MASTER_PROCNAME parameter between the Query Monitor subsystem and the Workload Replay DB2 subsystem, or the Security Guardium S-TAP for DB2 ASC started task.

User response

Update the MASTER_PROCNAME parameter for DB2 Query Monitor, Security Guardium S-TAP for DB2, or Workload Replay so that the same MASTER_PROCNAME is in use by all products for the monitored DB2 subsystem. After updating the MASTER_PROCNAME, restart the started task for the task that is affected by the parameter change.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3402I ISSUING COMMAND *cmd*

Explanation

Indicates command execution.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3551E VSAM LOGIC ERROR ENCOUNTERED WHILE ACCESSING CONTROL FILE FOR DB2® *ssid*. VSAMRC='*rc*' VSAMRS=X'*rs*'

Explanation

A VSAM logic error was encountered when accessing the control file for the DB2 subsystem indicated in the message.

User response

Verify that the DB2 control file for the DB2 subsystem listed in the message has been properly allocated and that the appropriate DB2 subsystem and plan names information have been specified correctly.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3552E SETUP INFORMATION MISSING FROM CONTROL FILE FOR DB2® *ssid*

Explanation

There is insufficient information in the control file for the DB2 subsystem indicated in the message.

User response

Modify the control file to include the necessary information.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ3553E *message* ERROR *message*

Explanation

An error has occurred. This message is customized to display various messages such as initialization errors.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ4001E CONNECT TO DB2® *ssid* FAILED FOR PLAN *plan* RETURN CODE *rc* REASON CODE *rs*

Explanation

Security Guardium® S-TAP® for DB2 was not able to connect to the DB2 subsystem using the plan shown in the message.

User response

Refer to *DB2 Universal Database for z/OS® V8 Messages* (GC18-9602-01) and *DB2 Universal Database for z/OS V8 Codes* (GC18-9603-01) to further diagnose and resolve the problem.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ4003E CONNECT FAILED - DB2® NOT OPERATIONAL

Explanation

The collector agent was not able to connect to the DB2 subsystem because DB2 is not currently operational.

User response

Verify that DB2 is functioning correctly.
Parent topic: Error messages and codes: ADHQxxxx

ADHQ5010I MONITORING AGENT DEINSTALLATION IN PROGRESS FOR SUBSYSTEM *ssid*

Explanation

The monitoring agent deinstallation is in progress for the DB2® subsystem indicated in the message.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ5011I MONITORING AGENT DEINSTALLATION COMPLETE FOR SUBSYSTEM *ssid*

Explanation

The monitoring agent deinstallation completed for the DB2® subsystem indicated in the message.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ5012I REQURESTING MONITORING AGENT ACTIVATION FOR DB2® SUBSYSTEM *ssid*

Explanation

The monitoring agent for the indicated DB2 subsystem is being requested for activation.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ5013I REQUESTING MONITORING AGENT DEACTIVATION FOR DB2® SUBSYSTEM *ssid*

Explanation

The monitoring agent for the indicated DB2 subsystem is being requested for deactivation.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ6101E LOCATE FAILED FOR *dataset* R0=*code* RC=*rc*

Explanation

A catalog located failed during interval data set expiration processing. r0 contains the contents of the register zero and rc is the LOCATE return code.

User response

See *z/OS® DFSMSdfp Advanced Services* (SC26-7400-02) for a description of the return codes issued by LOCATE.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ6102E SCRATCH FAILED FOR *file* SCRATCH STATUS CODE=*code* RO=*ro*

Explanation

The scratch failed for the indicated file.

User response

See *z/OS® DFSMSdfp Advanced Services* (SC26-7400-02) for a description of the return codes issued by LOCATE.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ7001E *table* TABLE NOT LOCATED IN DB2® CATALOG

Explanation

The table indicated in the message cannot be found in the DB2 catalog.

User response

Verify that the table you specified exists.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ7008E QUERY COMMON COLLECTOR *ssid* NOT VALID OR HAS NOT BEEN STARTED SINCE IPL

Explanation

The collector agent shown in the message is not a valid collector agent.

User response

Verify that you specified the correct Query Common Collector subsystem ID, and that the collector agent is available.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ7009E OUT OF SPACE CONDITION DETECTED WHILE WRITING TO THE *dsn* DATASET

Explanation

An out-of-space condition was encountered when attempting to write to the data set indicated in the message.

User response

Verify that adequate space has been allocated to the data set.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ7010E MISSING "ADD" PARAMETER FOR *parameter* AT LINE *line* COLUMN *column*

Explanation

The ADD parameter is missing for the indicated line and column.

User response

Specify an ADD parameter.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ7011E INTERNAL ERROR - UNABLE TO RESOLVE ALTERNATE COLUMN *column*

Explanation

There has been an internal error.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ7015E NUMBER OF BSDS SPECIFICATIONS INVALID OR MISSING

Explanation

An invalid number of BSDS parameters has been sent as input to the ADH#CTLF utility.

User response

Verify that the two boot strap data sets used for your DB2® subsystem are properly specified.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ7016E DUPLICATE RECORD STORE ATTEMPTED FOR DB2® SUBSYSTEM *ssid*

Explanation

This message describes an error condition when attempting to load records into the control file that already exist without specifying REPLACE(Y) for the DB2 subsystem indicated in the message.

User response

Edit your ADH#CTLF job to include REPLACE(Y). Refer to the instructions in SADHSAMP library member ADH#CTLF for details.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8001E ERRORS DETECTED IN *parameters* PARAMETERS:

Explanation

Errors have been detected in ADHCFGP.

User response

Verify that the parameters you specified in ADHCFGP are correct and modify any syntax errors before proceeding.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8002E UNIDENTIFIED KEYWORD DETECTED AT LINE *line* COLUMN *column*

Explanation

An unknown keyword has been found.

User response

Verify the correct syntax and modify the keyword as needed.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8003E INVALID SYNTAX SPECIFIED FOR *parameter* NEAR LINE *line* COLUMN *column*

Explanation

The syntax specified for the parameter indicated in the message is not valid.

User response

Correct the syntax and resubmit the job.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8004E PARAMETER LENGTH EXCEEDED FOR *parameter* NEAR LINE *line* COLUMN *column*

Explanation

The length of the value specified for the parameter indicated in the message exceeded the valid length for that parameter.

User response

Correct the syntax and resubmit the job.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8005E PARAMETER MISSING FOR *parameter* NEAR LINE *line* COLUMN *column*

Explanation

A required parameter is missing from ADHLOADP.

User response

Correct the syntax and resubmit the job.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8006E NON NUMERIC DATA SPECIFIED FOR *parameter* NEAR LINE *line* COLUMN *column*

Explanation

Non-numeric data was specified in ADHLOADP for the parameter listed in the message.

User response

Specify numeric data for the parameter.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8007E INVALID VALUE SPECIFIED FOR *parameter* NEAR LINE *line* COLUMN *column*

Explanation

An invalid value was specified in ADHLOADP.

User response

Correct the value and resubmit the job.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8008E *value* MUST BE *value* THAN *value*

Explanation

The value of the parameter shown in the message must be within the specified range.

User response

Correct the value of the parameter so it falls within the range indicated in the message text.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8009E DUPLICATE PARAMETER *parameter* AT LINE *line* COLUMN *column*

Explanation

A parameter you specified is a duplicate.

User response

Correct the syntax to eliminate the duplicate parameter.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8010E DUPLICATE SUBPARAMETER DETECTED FOR PARAMETER *parameter* AT LINE *line* COLUMN *column*

Explanation

A sub-parameter you specified is a duplicate.

User response

Correct the syntax to eliminate the duplicate sub-parameter.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8011E DB2® VERSION NOT SUPPORTED

Explanation

The version of DB2 with which you are attempting to use is not supported by unload functionality of the collector agent.

User response

The collector agent unloads data to DB2 Version 8, DB2 Version 9, or DB2 Version 10.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8012E ERROR OPENING DDNAME *ddname*

Explanation

The collector agent encountered an error attempting to open the TEXTDATA data set.

User response

Verify that the TEXTDATA data set is configured properly and has adequate space available.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8013E INVALID PARAMETER LENGTH FOR *parameter*

Explanation

The value you specified for the TBCREATOR parameter is too long and is therefore invalid.

User response

Specify a valid value for TBCREATOR. Valid values are up to eight characters in length.

Parent topic: Error messages and codes: ADHQxxxx

ADHQ8014E LOGIC ERROR: *error*

Explanation

The collector agent has encountered a logic error.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: ADHQxxxx

ADH8022I *adh parameter value*

Explanation

This message is used to display the contents of the ADHPARMS file that was processed when Security Guardium® S-TAP® for DB2® was started.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

ADH9899I *adh modify command*

Explanation

This message is used to display the text of a modify command that was issued to Security Guardium® S-TAP® for DB2®.

User response

No action is required.

Parent topic: Error messages and codes: ADHQxxxx

IBM Security Guardium S-TAP for IMS on z/OS

These topics describe how to use IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 (also referred to as IBM Guardium S-TAP for IMS). The V10.1.3 S-TAP is optimized for the V10.1 Guardium system. IBM Guardium S-TAP for IMS collects and correlates data access information from a variety of IMS resources to produce a comprehensive view of business activity for auditors.

About these topics

This information is designed to help database administrators, appliance programmers, and application programmers perform these tasks:

- Plan for the installation of IBM Guardium S-TAP for IMS
- Install and operate IBM Guardium S-TAP for IMS
- Configure the IBM Guardium S-TAP for IMS environment
- Diagnose and recover from IBM Guardium S-TAP for IMS problems

A PDF of this User's Guide is available here.

- **IBM Security Guardium S-TAP for IMS on z/OS**
  These topics describe how to use IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 (also referred to as IBM Guardium S-TAP for IMS). The V10.1.3 S-TAP is optimized for the V10.1 Guardium system. IBM Guardium S-TAP for IMS collects and correlates data access information from a variety of IMS resources to produce a comprehensive view of business activity for auditors.
- **What does IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 do?**
  IBM Security Guardium S-TAP for IMS on z/OS (also referred to as IBM Guardium S-TAP for IMS) is an auditing tool that collects and correlates data access information from IMS Online regions, IMS batch jobs, IMS archived log data sets, and SMF records to produce a comprehensive view of business activity that occurs within one or more IMS environments.
- **Installing IBM Security Guardium S-TAP for IMS on z/OS**
  The following sections describe hardware, software, and user ID authority prerequisites for product installation.
- **IBM Security Guardium S-TAP for IMS on z/OS security**
  IBM Guardium S-TAP for IMS requires access to various IMS data sets and IBM Guardium system components.
- **Configuration overview**
  These actions are required to configure IBM Guardium S-TAP for IMS.
- **Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent**
  This section describes the information necessary for configuring the agent.
- **Setting up an IMS environment for auditing**
  This section describes how to customize IMS environments to capture DLI calls, including customizing IMS catalogued procedures, coexisting with other DFSFLGX0 and DFSISVI0 exit routines, customizing IMS to use a zIIP, copying common load modules from SAUILOAD to SAUIIMOD, and the security considerations related to IMS processing.
- **Using agent configuration keywords to customize auditing**
  Some agent configuration keywords must be used for the product to function. You can also use agent configuration keywords for optional auditing specifications.
- **IBM Security Guardium S-TAP for IMS on z/OS agent reference information**
  The IBM Guardium S-TAP for IMS agent provides access to database and appliance services, in support of the product's remote clients. The agent also reads audited DLI events placed in the z/OS System Logger log streams by the IMS Online and DLI/DBB batch Data collectors and sends the DLI events to the IBM Guardium system using TCP/IP connections.
- **Data collection**
  The collection process involves the gathering of audit event data at run time. Specify various filtering criteria to capture all relevant events and limit the amount of data that is collected and stored.
- **Creating and modifying IMS definitions**
  An IMS definition establishes a connection from your Guardium system to the IMS environment that you want to audit. To create and modify IMS definitions from the Guardium system interface, the agent address space (AUIA*STC*) must have a preestablished connection to the Guardium system.
- **Reference information**
  This chapter provides IBM Guardium S-TAP for IMS reference information.
- **Troubleshooting**
  Use the following topics to diagnose and correct problems that you experience with IBM Guardium S-TAP for IMS.

Parent topic: S-TAP for z/OS V10.1.3 User's Guide
Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

What does IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 do?

IBM Security Guardium S-TAP for IMS on z/OS (also referred to as IBM Guardium S-TAP for IMS) is an auditing tool that collects and correlates data access information from IMS Online regions, IMS batch jobs, IMS archived log data sets, and SMF records to produce a comprehensive view of business activity that occurs within one or more IMS environments.

IBM Guardium S-TAP for IMS assists auditors in determining who read or updated a particular IMS database and its associated data sets, what mechanism was used to perform that action, and when the access took place.

IBM Guardium S-TAP for IMS can collect and correlate many different types of information, including:

- Accesses to databases and segments from IMS Online regions.
- Accesses to databases and segments from IMS DLI/DBB batch jobs.
- Accesses to databases, image copies, IMS logs, and RECON data sets and security violations to these data sets as recorded by SMF.
- IMS Online region START and STOP, database, and PSB change of state activity and user signon and signoff as recorded in the IMS Archived Log data sets.

Restriction: IBM Guardium S-TAP for IMS supports auditing of Data Entry Databases (DEDBs) and IMS Full Function databases. Auditing of Main Storage Databases (MSDBs) is not supported.

- **What's new in IBM Security Guardium S-TAP for IMS on z/OS V10.1.3?**
  Here's what's new in version 10.1.3 of IBM Guardium S-TAP for IMS.
- **IBM Guardium S-TAP for IMS components**
  IBM Guardium S-TAP for IMS consists of an agent, a Common Storage Management Utility, and the IBM Guardium system.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

What's new in IBM Security Guardium S-TAP for IMS on z/OS V10.1.3?

Here's what's new in version 10.1.3 of IBM Guardium S-TAP for IMS.

Enhancements to this version include:

- Echoing of active policy XML as described in Echoed XML statement definitions.
- Increased security of online and batch log streams as described in z/OS log streams.
- Filtering of DLI called based on IMS LTERM names
- Collection of the accessed HALDB PARTITION name during DLI call processing
- Check agent status without accessing z/OS by using a Guardium interface command
- Ability to enable simulation mode to simulate mainframe activity levels, test deployment, and gauge appliance requirements without sending data to the Guardium appliance
- New parameters to simplify audit record validation, debugging, and agent configuration
- Simplified agent configuration:
  - Complete SMF configuration is no longer required if the SMF_CYCLE_INTERVAL(0) parameter is specified in the AUICONFG file and SMF processing is disabled.
  - Complete IMSL configuration is no longer required if the IMSL_CYCLE_INTERVAL(0) parameter is specified in the AUICONFG file and IMSL processing is disabled.
- Messages AUII050I and AUIJ250I now include the IMSID to help identify which IMS system issued the message.
- Reduced CPU consumption and greater reliability during processing of IMS DLI calls in IMS online environments.
- RECON data sets that are read by the SMF (AUIF*STC* and IMS SLDS (AUIL*STC*) can optionally be copies of the live IMS RECON data sets.
- Option to disable DLI call auditing of IMS online DLI calls that originate from the following IMS region types: AER, BMP, CICS®, DBCTL, IFP, MPP, and ODBA.
- Support for Internet Protocol version 6 (IPV6) introduced with PH16991

Parent topic: What does IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 do?

IBM Guardium S-TAP for IMS components

IBM Guardium S-TAP for IMS consists of an agent, a Common Storage Management Utility, and the IBM Guardium system.

- **IBM Guardium system**
  The IBM Guardium system can gather and report information from multiple agents running on multiple z/OS systems.
- **IBM Guardium S-TAP for IMS agent**
  The IBM Guardium S-TAP for IMS agent coordinates the collection of audited data, and the transmission of audited DLI call data to the IBM Guardium system.

Parent topic: What does IBM Security Guardium S-TAP for IMS on z/OS V10.1.3 do?

IBM Guardium system

The IBM Guardium system can gather and report information from multiple agents running on multiple z/OS systems.

Note: In environments where multiple agents connect to a common IBM Guardium system or appliance, the z/OS agent started task names (AUIAS*TC*, AUILS*TC*, AUIFS*TC*) must be unique. Unique started task names enable the IBM Guardium S-TAP for IMS policies that are pushed from the IBM Guardium system to be attributed to, and monitored by, the correct z/OS agent.

IBM Guardium system components

The IBM Guardium system:

- Provides the user interface, which processes requests and displays the resulting information.
- Enables you to create collection policies, which specify the types of data to be collected by the agent.
- Stores the collected data.

IBM Guardium system and S-TAP agent communication

The IBM Guardium system and the IBM Guardium S-TAP for IMS agent communicate using a TCP/IP connection. The policies you create, using the user interface, tell the agent what data to collect. The policy specifies filter information, such as which data sets are to be monitored for data accesses.

Parent topic: IBM Guardium S-TAP for IMS components

IBM Guardium S-TAP for IMS agent

The IBM Guardium S-TAP for IMS agent coordinates the collection of audited data, and the transmission of audited DLI call data to the IBM Guardium system.

The IBM Guardium S-TAP for IMS agent can collect data from one or more of the following sources within a SYSPLEX:

- A single IMS system
- Multiple IMS systems that share a common set of RECON data sets
- Multiple IMS systems using diverse RECON data sets

The agent maintains the communication links that are needed to exchange information with:

- The IBM Guardium system
- IMS Online and Batch data collectors and activity monitors
- The IMS Archive Log data set and SMF activity monitors

The agent also provides data collection schemas, called policies, to the activity monitors on which detail the IMS artifacts are to be audited, and to what level.

The agent runs as a started task on the z/OS host. An example of the JCL to be used is in member AUIASTC of the SAUISAMP installation data set.

The agent collects data from the following sources:

- IMS online activities
- IMS batch activities
- SMF data
- IMS archived log data
- IMS RECON data sets

For more information about how data is collected from these sources, see Data collection monitors.
Parent topic: IBM Guardium S-TAP for IMS components

Installing IBM Security Guardium S-TAP for IMS on z/OS

The following sections describe hardware, software, and user ID authority prerequisites for product installation.

Review the IBM Guardium S-TAP for IMS V10.1.3 Program Directory for a list of product materials and SMP/E installation instructions.

- **Hardware and software prerequisites**
  The following hardware and software are required to operate IBM Guardium S-TAP for IMS V10.1.3.
- **User ID authorities that are required for installation**
  The following z/OS USERID authorities are needed to install IBM Guardium S-TAP for IMS.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Hardware and software prerequisites

The following hardware and software are required to operate IBM Guardium S-TAP for IMS V10.1.3.

- z/OS Version 2 Release 2 or later, until end of service.
- IMS V13 -- V15, until end of service.
- Any hardware capable of running z/OS Version 2 Release 1 or later, until end of service.

IBM Guardium S-TAP for IMS requires use of the following:

- 64-bit memory
- TCP/IP connectivity
- z/OS System logger log streams
- UNIX System Services
- OMVS segment

Parent topic: Installing IBM Security Guardium S-TAP for IMS on z/OS

User ID authorities that are required for installation

The following z/OS USERID authorities are needed to install IBM Guardium S-TAP for IMS.

If you are installing this product, your z/OS user ID must have the authority to:

- Define z/OS system log streams
- Update the IMS cataloged procedure data set members DLIBATCH and DBBBATCH to include product load libraries

Parent topic: Installing IBM Security Guardium S-TAP for IMS on z/OS

IBM Security Guardium S-TAP for IMS on z/OS security

IBM Guardium S-TAP for IMS requires access to various IMS data sets and IBM Guardium system components.

- **APF authorization**
  IBM Guardium S-TAP for IMS requires certain data sets to be accessible and APF-authorized on all LPARS of the SYSPLEX where IMS batch jobs or monitored IMS online regions might run.
- **OMVS segment**
  TCP/IP connectivity and other UNIX System services on z/OS require that the address space that is using these services use a z/OS user ID or group name that is defined with an OMVS segment.
- **TCP/IP connections**
  IBM Guardium S-TAP for IMS uses Transmission Control Protocol/Internet Protocol (TCP/IP) to connect to the Guardium appliance. To enable this communication, make sure you have the correct permissions assigned.
- **z/OS log streams**
  IBM Guardium S-TAP for IMS monitors the IMS batch jobs and online regions and writes audit data to z/OS log streams.
- **IMS RESLIB data sets**
  READ access to the IMS RESLIB/SDFSRESL data sets is required for each IMS system that requires the IMS SLDS to be processed by IBM Guardium S-TAP for IMS. READ access is required to allow a LOAD/READ of module DFSVC000 to determine the version release level of the audited IMS.
- **SMF and IMS archive log data sets**
  READ access to the SMF data sets and the IMS archived logs data sets (SLDS) is required for the user under whose authority the agent runs. If these data sets are protected by RACF® or another security product, a policy must be defined to grant this access. The z/OS catalogs containing the names of these data sets, as well as the physical data sets themselves, must be accessible from the LPAR on which the IBM Guardium S-TAP for IMS agent runs.
- **DBRC RECON data sets**
  IBM Guardium S-TAP for IMS uses the native VSAM services to read data from the RECON data sets. These RECON data sets must be accessible from all the LPARS where the IBM Guardium S-TAP for IMS agents might run.
- **Operator commands**
  You can use z/OS Operator commands, to start IBM Guardium S-TAP for IMS tasks.
- **Quarantining Database DLI calls**
  IBM Guardium S-TAP for IMS enables you to quarantine the DB DLI calls of specific users for specific periods of time.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

APF authorization

IBM Guardium S-TAP for IMS requires certain data sets to be accessible and APF-authorized on all LPARS of the SYSPLEX where IMS batch jobs or monitored IMS online regions might run.

About this task

Refer to the *z/OS Knowledge Center* for more information about how to APF authorize libraries.

Procedure

1. APF-authorize product data set SAUILOAD on all LPARS of the SYSPLEX.
   SAUILOAD contains the IMS Online and Batch Activity Monitor executable code.
2. APF-authorize product data set SAUIIMOD on all LPARS of the SYSPLEX where IMS batch jobs or IMS online regions to be monitored might run.
   SAUIIMOD contains IMS specific executable load modules.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

OMVS segment

TCP/IP connectivity and other UNIX System services on z/OS require that the address space that is using these services use a z/OS user ID or group name that is defined with an OMVS segment.

Defining your z/OS user ID or group name with an OMVS segment might require the use of the IBM RACF command ADDUSER/ALTUSER xxxxxx OMVS(UID(zzz)) or a security product equivalent command. Review your z/OS Security Server documentation for more information.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

TCP/IP connections

IBM Guardium S-TAP for IMS uses Transmission Control Protocol/Internet Protocol (TCP/IP) to connect to the Guardium appliance. To enable this communication, make sure you have the correct permissions assigned.

If you are working from a secure communications port, enable the user ID that is associated with the agent started task to have READ/WRITE permissions on the ports that are assigned to the agent.

See Using agent configuration keywords to customize auditing for more information about the ADS_LISTENER_PORT, APPLIANCE_PORT, and LOG_PRT_SCAN_START configuration keywords.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

z/OS log streams

IBM Guardium S-TAP for IMS monitors the IMS batch jobs and online regions and writes audit data to z/OS log streams.

The IBM Guardium S-TAP for IMS Online and DLI/DBB batch data collectors audit DLI events that occur in the IMS Online and DLI/DBB Batch regions. Audited DLI events are written to z/OS System Logger log streams, which are then read by the IBM Guardium S-TAP for IMS agent. The IMS agent sends the audit data to the IBM Guardium appliance by using TCP/IP connections.

To permit the IMS Online and DLI/DBB batch collectors to write to the log streams, systems authorization facility (SAF) security access of UPDATE to the z/OS log stream is required for all user IDs associated with the audited IMS Control region and DLI/DBB batch jobs that might cause IMS DLI calls to be audited.

You can now use an additional SAF resource to further secure the online and batch log streams. For example, you can now prevent the log streams from being read by a user program or utility that is initiated by a user who is authorized to update to the log stream. Apply z/OS V2R3 and V2R4 APAR OA56050 to optionally add an additional authority check for a SAF profile that covers resource (WRITE_ONLY_log-stream-name) in class LOGSTRM. This new profile option enables you to limit users to only connecting to (IXGCONN REQUEST=CONNECT), writing to (IXGWRITE), and disconnecting from (IXGCONN REQUEST=DISCONNECT) the log stream. Other IXG calls, such as IXGBRWSE (read), are rejected with return code 8 and reason code '081C'x. For more information, refer to the documentation provided in the HOLD data for APAR OA56050.

Note: User IDs that are associated with the IBM Guardium S-TAP for IMS agent must have authority to read and delete data from the log stream and should not be limited by using resource (WRITE_ONLY_log-stream-name). Log stream UPDATE authority is recommended for the IBM Guardium S-TAP for IMS agents.
Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

IMS RESLIB data sets

READ access to the IMS RESLIB/SDFSRESL data sets is required for each IMS system that requires the IMS SLDS to be processed by IBM Guardium S-TAP for IMS. READ access is required to allow a LOAD/READ of module DFSVC000 to determine the version release level of the audited IMS.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

SMF and IMS archive log data sets

READ access to the SMF data sets and the IMS archived logs data sets (SLDS) is required for the user under whose authority the agent runs. If these data sets are protected by RACF® or another security product, a policy must be defined to grant this access. The z/OS catalogs containing the names of these data sets, as well as the physical data sets themselves, must be accessible from the LPAR on which the IBM Guardium S-TAP for IMS agent runs.

Consult your security administrator to determine what is currently protected and how to grant the required access.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

DBRC RECON data sets

IBM Guardium S-TAP for IMS uses the native VSAM services to read data from the RECON data sets. These RECON data sets must be accessible from all the LPARS where the IBM Guardium S-TAP for IMS agents might run.

VSAM access to the RECON data sets is READ-ONLY, allowing the IBM Guardium S-TAP for IMS jobs and started tasks with a security access of READ to process the RECON data sets.

Consult your security administrator to determine how your RECON data sets are protected, and how to grant the required access.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

Operator commands

You can use z/OS Operator commands, to start IBM Guardium S-TAP for IMS tasks.

The user ID that is assigned to the IBM Guardium S-TAP for IMS agent started task must be permitted to issue START commands to initiate the AUIF*stc*, AUIL*stc*, and AUIU*stc* tasks. During installation, administrators can configure the z/OS security product to restrict users and programs from issuing z/OS Operator commands.
Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

Quarantining Database DLI calls

IBM Guardium S-TAP for IMS enables you to quarantine the DB DLI calls of specific users for specific periods of time.

Quarantining a user of a specific IMS subsystem means that for the specified time period, the quarantined user is not able to run DB DLI calls either by using the targeted IMS subsystem, or while running DLI/DBB batch jobs.

If a quarantined user attempts access during a restricted time, the DLI call is not performed, and a status code of `AI` is returned in the DBPCB status code field.

To create quarantine rules, access the Policy Builder from the Tools and Views section of the Guardium appliance interface Setup menu.

Note:

- DLI calls that are made to IMS Fast Path databases by using IMS Fast Path exclusive transactions or BMPs cannot be quarantined.
- Quarantine does not take effect immediately. The audited DLI call that produces the event to trigger the quarantine is completed before the quarantine takes effect. It is possible for DLI calls to be run by the quarantined user before the quarantine takes effect.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS security

Configuration overview

These actions are required to configure IBM Guardium S-TAP for IMS.

Review the following steps, which are described in greater detail in the following sections:

- Verify that you have the resource authorizations that are required to configure the product.

- Review the steps to plan your configuration and customize your environment.
- Set up the z/OS log streams. Review the CFRM and log stream size requirements, and the related security considerations, limitations, and restrictions. Define the log streams for batch and online jobs.
- Determine a naming convention for the agent (AUIA*STC*, AUIF*STC*, AUIL*STC*, and AUIU*STC*) started tasks, where *STC* can be changed to any 1 - 4 character length string.
  Tip: Retain the AUI prefix to simplify task identification.
- Configure the agent by customizing the configuration file, customizing the agent JCL, and starting the agent.
- Set up the IMS environment for auditing by customizing the IMS cataloged procedure, configuring IMS exits, customizing IMS to use an IBM System z® Integrated Information Processor (zIIP), and review the related security considerations.

Note: No WLM (Workload Manager) considerations are necessary. All agent started tasks use the STC WLM class.

- **Upgrading from Guardium S-TAP for IMS V9.0**
  Complete the following steps to upgrade from InfoSphere® Guardium S-TAP for IMS V9.0 to IBM Guardium S-TAP for IMS V10.1.3. These steps enable V9.0 product assets, such as JCLs and configuration and repository contents, to be upgraded to V10.1.3, while allowing the full use and functionality of the V10.1.3 product.
- **Upgrading from Guardium S-TAP for IMS V9.1 or V10.0**
  The agent JCL and configuration file that are used by IBM Guardium S-TAP for IMS V9.1 and V10.0 are compatible with IBM Guardium S-TAP for IMS V10.1.3. No configuration changes are required to upgrade from IBM Guardium S-TAP for IMS V9.1 to IBM Guardium S-TAP for IMS V10.1.3.
- **Planning your configuration and customizing your environment**
  Collect user ID and environment information before you configure IBM Guardium S-TAP for IMS V10.1.3.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Upgrading from Guardium S-TAP for IMS V9.0

Complete the following steps to upgrade from InfoSphere® Guardium S-TAP for IMS V9.0 to IBM Guardium S-TAP for IMS V10.1.3. These steps enable V9.0 product assets, such as JCLs and configuration and repository contents, to be upgraded to V10.1.3, while allowing the full use and functionality of the V10.1.3 product.

Before you begin

New versions or releases of IBM Guardium S-TAP for IMS should be installed as a new installation base. However, if circumstances prevent you from doing so, follow these instructions to upgrade from the previous version's installation base.

Procedure

1. Deactivate or uninstall all policies that apply to the agent that you are upgrading.
2. Shut down the agent that you are upgrading.
3. Customize the AUIMIG10 SAMPLIB member to convert the configuration file and repository to V10.1.3 format, and submit.
   The comments that are contained in the AUIMIG10 SAMPLIB member describe how to customize the JCL. A V10.1.3 format configuration file, and an IMS definition report will be produced.
4. Use the IMS definition report, which is produced by the AUIMIG10 utility, to add the IMS definitions to your IBM Guardium system.
5. Update the new configuration file, which is produced by the AUIMIG10 utility, with any changes.
6. Update the AGENT (AUIA*STC*) and Memory Management Utility (AUIU*STC*) JCLs as follows:
   a. Remove the //AUICFG DD JCL statement.
   b. Add a //AUICONFG DD JCL statement, and set it to reference the new configuration member produced by the AUIMIG10 utility.
   c. Change the //STEPLIB DD JCL statement to reference the V10.1.3 product load library (SAUILOAD).
   d. Remove the //AUIREPOS DD JCL statement from the AUIU*STC* JCL.
7. Update the SMF (AUIF*STC*) and IMS Archive Log (AUIL*STC*) JCLs as follows:
   a. Remove the //AUICFG DD JCL statement, and any procedure parameters that reference it.
   b. Change the //STEPLIB DD JCL statement to reference the V10.1.3 product load library (SAUILOAD).
8. Update the IMS Control region JCLs that are audited by the agent to use the V10.1.3 product IMS load library (SAUIIMOD).
9. Update the IMS DBBBATCH and DLIBATCH cataloged procedures, and any equivalent JCL members, to use the V10.1.3 product IMS load library (SAUIIMOD).
10. Start the agent.
11. Install or activate the policies that you want to apply.
12. Stop and restart your IMS systems.

What to do next

Now, you can:

- Install additional policies on the z/OS host by using the IBM Guardium system user interface.
- Manage agent and IMS definitions by using the IBM Guardium system user interface.

Note: The format of the data that is written to the z/OS logstreams has changed from V9.0 to V10.1.3. IBM Guardium S-TAP for IMS V10.1.3 converts any existing V9.0 data from existing logstreams to a usable format. If you migrate from a V10.1.3 system back to a V9.0 system, you must reinitialize the z/OS log streams before restarting InfoSphere Guardium S-TAP for IMS V9.0.

Parent topic: Configuration overview

Upgrading from Guardium S-TAP for IMS V9.1 or V10.0

The agent JCL and configuration file that are used by IBM Guardium S-TAP for IMS V9.1 and V10.0 are compatible with IBM Guardium S-TAP for IMS V10.1.3. No configuration changes are required to upgrade from IBM Guardium S-TAP for IMS V9.1 to IBM Guardium S-TAP for IMS V10.1.3.

Before you begin

Do not attempt to run AUIMIG10 to upgrade from Guardium S-TAP for IMS V9.1 or V10.0 to IBM Guardium S-TAP for IMS V10.1.3.

About this task

The format of the data that is written to the z/OS logstreams has changed in V10.1.3. IBM Guardium S-TAP for IMS V10.1.3 converts any existing Guardium S-TAP for IMS V9.1 and V10.0 data from existing logstreams to a usable format. If you migrate from a V10.1.3 system back to a V9.1 or V10.0 system, you must reinitialize the z/OS log streams before restarting the previous product version.
Parent topic: Configuration overview

Planning your configuration and customizing your environment

Collect user ID and environment information before you configure IBM Guardium S-TAP for IMS V10.1.3.

Tip: To upgrade to IBM Guardium S-TAP for IMS from a previous version, refer to the appropriate topic:

- Upgrading from Guardium S-TAP for IMS V9.0
- Upgrading from Guardium S-TAP for IMS V9.1 or V10.0

If you are upgrading from a previous version to V10.1.3, no further configuration steps are required. Upgrading to V10.1.3 requires the use of, and modifications to, the same agent name and JCLs that were used with previous versions. For your reference, see the Sample library members table.
Before you configure a new installation of IBM Guardium S-TAP for IMS V10.1.3, determine the following:

- The user IDs that will be used to run the agent started tasks
- Where the agent started tasks will run

Then, customize the ISPF edit macro, review the job card requirement, and set up the z/OS log streams, as described in the following sections.

- **Customizing the ISPF edit macro**
  The SAUISAMP data set shipped with IBM Guardium S-TAP for IMS includes an ISPF edit macro to help with the editing of the rest of the SAMPLIB members to be used in the subsequent steps.
- **Job cards for the sample JCL in the SAMPLIB**
  Some JCL members included with the product SAMPLIB have a filler card for the job card.
- **Setting up z/OS log streams**
  IBM Guardium S-TAP for IMS uses the z/OS System Logger to funnel events from IMS online regions and DLI/DBB batch jobs to the DLI event processor (AUIA*STC* task). Both XCF based and DASD based log streams are supported.

Parent topic: Configuration overview

Customizing the ISPF edit macro

The SAUISAMP data set shipped with IBM Guardium S-TAP for IMS includes an ISPF edit macro to help with the editing of the rest of the SAMPLIB members to be used in the subsequent steps.

About this task

The edit macro is named AUIEMAC1 and provides a straightforward way to customize the variable values for the variables that appear in the JCL that will run. Use this edit macro as part of a command list (CLIST) to edit the other SAMPLIB members.

Procedure

1. To set up the edit macro, copy AUIEMAC1 from the #HLQ.SAUISAMP to a CLIST library.
2. Edit the macro by providing the appropriate values for each of the variables.
3. To run the macro, type the name of the edit macro in the command line in ISPF.

Results

After you modify the edit macro, you can use it as a command to customize other SAMPLIB members in the following steps, unless otherwise specified.

Example

The contents of the edit macro AUIEMAC1 included in the SAMPLIB are as follows:

```
ISREDIT MACRO (NP)
ISPEXEC VGET (ZUSER)
ISREDIT CHANGE ALL '#AUILOAD'           AUI.IBMTAPE.SAUILOAD
ISREDIT CHANGE ALL '#AUIIMOD'           AUI.IBMTAPE.SAUIIMOD
ISREDIT CHANGE ALL '#AUISAMP'           AUI.IBMTAPE.SAUISAMP
ISREDIT CHANGE ALL '#AUICONFG'          AUICONFG
```

This table describes each variable in the edit macro AUIEMAC1 included in the SAMPLIB:

Table 1. AUIEMAC1 Edit macro variables

Variable	Default	Instructions
#AUILOAD	AUI.IBMTAPE.SAUILOAD	Change the default value to point to the location of the SAUILOAD for IBM Guardium S-TAP for IMS.
#AUIIMOD	AUI.IBMTAPE.SAUIIMOD	Change the default value to point to the location of the SAUIIMOD for IBM Guardium S-TAP for IMS.
#AUISAMP	AUI.IBMTAPE.SAUISAMP	Change the default value to point to the location of the SAUISAMP data set, or copy of that data set where you will be performing the configuration and customization edits.
#AUICONFG	AUICONFG	Change the default value to point to the member name in the configuration file that you want to use.

Parent topic: Planning your configuration and customizing your environment

Job cards for the sample JCL in the SAMPLIB

Some JCL members included with the product SAMPLIB have a filler card for the job card.

A valid job card conforming to your site's JCL standards must be provided before submitting any of the JCL.
Parent topic: Planning your configuration and customizing your environment

Setting up z/OS log streams

IBM Guardium S-TAP for IMS uses the z/OS System Logger to funnel events from IMS online regions and DLI/DBB batch jobs to the DLI event processor (AUIA*STC* task). Both XCF based and DASD based log streams are supported.

Each agent requires two unique log streams:

- one log stream for DLI events generated by IMS Control regions
- one log stream for DLI events generated by DLI/DBB batch jobs

Log streams cannot be shared between agents. Each log stream name must be unique.

It is recommended that XCF based log streams be used whenever possible, because this type of log stream is accessible from any LPAR within a sysplex, and has performance benefits. For more information about log streams, refer to the IBM publication: *System Programmer's Guide to: z/OS System Logger*.

- **Log stream security**
  Verify the following conditions have been met to insure log stream security.
- **XCF-based log streams**
  The advantages of using XCF-based log streams, as opposed to DASD-based log streams, include accessibility from any LPAR within the sysplex, and improved performance.
- **DASD-based log streams**
  This section provides rules and information about DASD-based log streams. Using DASD-based log streams limits auditing by the agent to the LPAR within which the agent is started. IMS Control regions and IMS DLI/DBB batch jobs that run on other LPARS will not be audited.

Parent topic: Planning your configuration and customizing your environment

Log stream security

Verify the following conditions have been met to insure log stream security.

Important:

- The USERID your IMS online control region runs under must have WRITE access to the log stream.
- If DLI/DBB batch jobs runs under a common USERID, that USERID must have WRITE permission to the log stream.
- The USERID under which the DLI Event Collector (AUIA*STC* task) executes must have READ/WRITE access to the log streams.
- If individual users are permitted to run DLI/DBB batch jobs under their own USERID, a universal access of WRITE is recommended for the log stream.

Parent topic: Setting up z/OS log streams

XCF-based log streams

The advantages of using XCF-based log streams, as opposed to DASD-based log streams, include accessibility from any LPAR within the sysplex, and improved performance.

AUILSTR1

Two JCL members in the SAUISAMP product data set are included to assist in the definition of XCF-based log streams.

This JCL is used to define the XCF structures to a CFRM policy needed by the log streams used by the DLI/DBB batch and IMS online control regions. Detailed instructions are in the comments of the JCL.
Note: The addition of structures to a CFRM policy are cumulative, and the execution of this JCL without consideration to previously defined structures within the CFRM policy result in the loss of existing CFRM structure definitions. It is highly recommended that a systems programmer customize and submit this JCL.

There are two DEFINE STRUCTURE sections for this JCL: one for the batch structure, and one for the online structure. The following values must be customized for the batch structure:

The name of the batch structure
    (NAME(batch_struc_name))
The coupling facility used to contain the structure
    (PREFLIST(cfname))

The following values must be customized for the online structure:

The name of the online structure
    (NAME(online_struc_name))
The coupling facility used to contain the structure
    (PREFLIST(cfname))

Do not change any other values, such as SIZE, INITSIZE, and ALLOWAUTOALT without carefully considering the impact that your changes will have on performance and data integrity.

Note:

- AUILSTR1 must run successfully before proceeding.
- When auditing in a large test or production environment, the INITSIZE and SIZE parameters can be increased to a higher value (example: 49200) for improved throughput.

AUILSTR2

This JCL is used to add the XCF based log streams to a LOGR policy used by the IMS Control region and DLI/DBB batch jobs. Detailed instructions are in the comments of the JCL.
Note: The addition of structures to a CFRM policy are cumulative, and the execution of this JCL without consideration to previously defined structures within the CFRM policy result in the loss of existing CFRM structure definitions. It is highly recommended that a systems programmer customize and submit this JCL.

There are two DEFINE STRUCTURE sections for this JCL: one for the batch structure and log stream, and one for the online structure.

Values that must be customized for IMS Batch processing include:
DEFINE STRUCTURE values:

The name of the batch structure (from AUILSTR1)
(NAME(batch_struc_name))

The name of this log stream is used as input to the Batch DLI Log Stream Name field when defining log streams to the agent. Use the LOG_STREAM_DLIB keyword of the configuration member that is specified by the AUICONFG DD statement of the agent (AUIA*STC*) JCL. The LOGSNUM, MAXBUFSIZE and AVGBUFSIZE should not be changed from the default values.

The name of the batch structure (from AUILSTR1)
(STRUCTNAME(batch_struc_name))
The selection of the Staging data set classes
(STG_DATACLAS, STG_MGMTCLAS, and STG_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates a staging data set for the log stream. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters.

The selection of offload data set classes
(LS_DATACLAS, LS_MGMTCLAS, and LS_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates an offload data set for the log stream. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters.

The size of the Batch Log stream DASD data sets
(STG_SIZE)
Note: This can be removed if the STG_DATACLAS value is specified.

The allocation/size of the offload data sets
(LS_SIZE(13500))

The default value is 13500 (the number of 4K blocks). The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of this size. When auditing in a large test or production environment, a value of 40500 might improve throughput.

The High level qualifier of the offload and staging data sets
(HLQ or EHLQ)

The HLQ and EHLQ are mutually exclusive and only one can be used. Other parameters found in the batch structure and online log stream definition might have a do not change comment. These parameters contain the recommended values and should not be altered without careful consideration of the impact of changes to log stream performance and data integrity. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter.

You must customize the following values for online structure and log stream processing:

DEFINE STRUCTURE values:

The name of the online structure (from AUILSTR1)
(NAME(online_struc_name))

The LOGSNUM, MAXBUFSIZE and AVGBUFSIZE should not be changed from the default values.
DEFINE LOGSTREAM values:

The name of the log-stream
(NAME(online_logstream_name))

The name of this log stream is used as input to the Online DLI Log Stream Name field when defining log streams to the agent. Use the LOG_STREAM_DLIO keyword of the configuration member specified by AUICONFG DD statement of the agent (AUIA*STC*) JCL.

The name of the online structure (from AUILSTR1)
(STRUCTNAME(online_struc_name))
The selection of the Staging data set classes
(STG_DATACLAS, STG_MGMTCLAS, and STG_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates a staging data set for the log stream. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter.

The size of the ONLINE Log stream DASD data sets
(STG_SIZE)
Note: This can be removed if the STG_DATACLAS value is specified.

The selection of offload data set classes
(LS_DATACLAS, LS_MGMTCLAS, and LS_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates an offload data set for the log stream. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter.

The allocation/size of the offload data sets
(LS_SIZE(13500))

The default value is 13500 (the number of 4K blocks). The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of this size. When auditing in a large test or production environment, a value of 40500 might improve throughput.

The High level qualifier of the offload and staging data sets
(HLQ or EHLQ)

The HLQ and EHLQ are mutually exclusive and only one can be used. Other parameters found in the batch structure and online log stream definition might have a do not change comment. These parameters contain the recommended values and should not be altered without careful consideration of the impact of changes to log stream performance and data integrity. The IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter.
Parent topic: Setting up z/OS log streams

DASD-based log streams

This section provides rules and information about DASD-based log streams. Using DASD-based log streams limits auditing by the agent to the LPAR within which the agent is started. IMS Control regions and IMS DLI/DBB batch jobs that run on other LPARS will not be audited.

DASD-based logs streams can only be accessed from one LPAR at a time. Any IMS Online Control regions and DLI/DBB batch jobs to be audited must run on the same LPAR as the agent runs on.

One JCL member in the SAUISAMP product data is included to assist in the definition of DASD-based log streams.

AUILSTR3

This JCL is used to add the DASD based log streams to a LOGR policy used by the IMS Control region and DLI/DBB batch jobs. Detailed instructions can be found within the comments of the JCL.
Note: It is highly recommended that a systems programmer customize and submit this JCL.
There are two DEFINE STRUCTURES sections to this JCL: one for the batch structure, and one for the online structure. Values which must be customized for IMS batch log stream processing are as follows:
DEFINE LOGSTREAM values:

The name of the log-stream
(NAME(batch_logstream_name))

The name of this log stream is used as input to the Batch DLI Log Stream Name field when defining log streams to the agent. Use the LOG_STREAM_DLIO keyword of the configuration member specified by AUICONFG DD statement of the agent (AUIA*STC*) JCL.

The selection of the Staging data set classes
(STG_DATACLAS, STG_MGMTCLAS and STG_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates a staging data set for the log stream. Other parameters found in the batch structure and online log stream definition might have a do not change comment. These parameters contain the recommended values and should not be altered without careful consideration of the impact of changes to log stream performance and data integrity. For more information, the IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters, and can be found on the IBM Information Center.

The selection of offload data set classes
(LS_DATACLAS, LS_MGMTCLAS and LS_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates an offload data set for the log stream. For more information, the IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters, and can be found on the IBM Information Center.

The size of the Batch Log stream DASD data sets
(STG_SIZE)
Note: This can be removed if the STG_DATACLAS value is specified.

The allocation/size of the offload data sets
(LS_SIZE(13500))

A value of 13500 (the number of 4K blocks) is the default/supplied value. For more information, the publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of this size, and can be found on the IBM Information Center.

The High level qualifier of the offload and staging data sets
(HLQ or EHLQ)

The HLQ and EHLQ are mutually exclusive and only one can be used. For more information, the IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter, and can be found on the IBM Information Center.

Values which must be customized for IMS ONLINE processing include the following:

DEFINE LOGSTREAM values:

The name of the log-stream
(NAME(online_logstream_name))

The name of this log stream is used as input to the Online DLI Log Stream Name field when defining log streams to the agent using the Guardium user interface.

The selection of the Staging data set classes

(STG_DATACLAS, STG_MGMTCLAS, and STG_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates a staging data set for the log stream. For more information, the IBM publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters, and can be found on the IBM Information Center.

The size of the ONLINE Log stream DASD data sets
(STG_SIZE)
Note: This can be removed if the STG_DATACLAS value is specified.

The selection of offload data set classes
(LS_DATACLAS, LS_MGMTCLAS, and LS_STORCLAS)

These parameters indicate the SMS classes to be used when the System logger allocates an offload data set for the log stream. For more information, the publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of these parameters, and can be found on the IBM Information Center.

The allocation/size of the offload data sets
(LS_SIZE(13500))

A value of 13500 (the number of 4K blocks) is the default/supplied value. For more information, the publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations for the choice of this size, and can be found on the IBM Information Center.

The High level qualifier of the offload and staging data sets
(HLQ or EHLQ)

The HLQ and EHLQ are mutually exclusive and only one can be used. Other parameters found in the batch structure and online log stream definition might have a do not change comment. These parameters contain the recommended values and should not be altered without careful consideration of the impact of changes to log stream performance and data integrity. For more information, the publication, *System Programmer's Guide to: z/OS System Logger* contains recommendations and considerations of each potential parameter, and can be found on the IBM Knowledge Center
Parent topic: Setting up z/OS log streams

Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent

This section describes the information necessary for configuring the agent.

The agent has a primary agent address space that runs as a started task (AUIA*STC*) and multiple secondary address spaces (AUIF*STC*, the SMF collector, AUIL*STC*, the IMS log collector, AUIU*STC*, the common storage utility) that are automatically started and stopped by the primary address space.

The agent primary address space reads the configuration file specified by the AUICONFG DD statement in the AUIA*STC* JCL, and passes the appropriate configuration information to the associated AUIF*STC* and AUIL*STC* tasks. The AUIU*STC* JCL requires the same configuration file to be specified as was specified for the AUIA*STC* task. Use the AUICONFG DD statement to specify the configuration file.

The SAUISAMP member AUICONFG provides a sample configuration that can be used by the agent primary address space started task.

Refer to the following instructions about the AUICONFG data set or the instructions in the data sets to complete the next steps.

Note:

- The data set must be edited using the EBCDIC encoding (1047 CCSID).
- It is recommended that you make a copy of the AUICONFG from SAUISAMP and customize it for use by a given agent.

- **Customizing the agent by using agent parameter keywords**
  Use agent parameter keywords to customize the agent. The agent configuration file provides the parameters that can be customized. The parameters that do not have a default value must be specified before you start the agent started task.
- **Agent configuration**
  The IP addresses of the IBM Guardium system appliances are specified using the SAUISAMP data set AUICONFG member using the APPLIANCE_SERVER and APPLIANCE_SERVER_FAILOVER_[1-5] keywords.
- **Customizing the agent JCL**
  The SAUISAMP member AUIA*STC* provides a sample JCL that can be used for the agent started task. This topic describes how to customize the JCL.
- **Starting and stopping the agent**
  Start the agent by issuing the command /S AUIASTC from the SDSF command line. The primary agent address space starts the AUIF*STC* address spaces. One or more instances of AUIL*STC* might also be started, depending on the list of active collections.
- **Agent security considerations**
  The user ID of the agent started tasks (the primary and the secondary started tasks) should have the necessary RACF® profiles for reading the configuration member contents.
- **Modifying the frequency of AUIJ012I messages**
  You can modify how frequently the agent provides a count of DLI calls (from the default of every 10K DLI calls to a value of your choice, 10K – 999K, 1M – 10M.)

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Customizing the agent by using agent parameter keywords

Use agent parameter keywords to customize the agent. The agent configuration file provides the parameters that can be customized. The parameters that do not have a default value must be specified before you start the agent started task.

How to use the agent parameters

- Use the AUICONFG DD statement to reference these parameters with the agent JCL (AUIA*STC*) and Memory Management secondary address space JCL (AUIU*STC*).
- The AUICONFG DD can be used in other agent secondary address space JCLs (AUIF*STC* and AUIL*STC*).
- Define the data set (DSORG=PS) or data set member (DSORG=PDS|PDS/E) that contains these parameters as RECFM=FB LREL=80.

- Specify only one keyword and parameter per line.
- An asterisk (*) or hyphen (-) in column one indicates that the line is a comment.
- Characters in column 72 and beyond are ignored.

Required parameters

The following parameters must be manually configured:

- APPLIANCE_SERVER
- LOG_STREAM_DLIB
- LOG_STREAM_DLIO
- SMF_DSN_MASK
- SMF_SPILL_FILE

All available agent parameters

ADS_SHM_ID

Required: No
Default: None
Description: This keyword is optional when only one agent exists in a sysplex environment. If more than one agent exists, the configuration file for each agent should have this keyword specified with a unique integer with a value of 100000 - 999999 specified as its parameter. This keyword identifies a shared memory segment that is specific to each agent.
Note:

- This keyword must be used in combination with ADS_LISTENER_PORT.
- If you specify this keyword, you must add an //AUICONFG DD statement to the AUIF*STC* and AUIL*STC* address space JCLs. This DD statement should point to the same data set and member as the agent AUIA*STC* and AUIU*STC* JCLs to enable communication between all participating address spaces.

Syntax: ADS_SHM_ID*(Shared_Memory_label)*
Example: ADS_SHM_ID(100010)

ADS_LISTENER_PORT

Required: No
Default: 39987
Description: This keyword is optional when only one agent exists in a sysplex environment. If more than one agent exists, the configuration file for each agent should have this keyword specified with a unique port number specified. This keyword identifies an agent-specific communications port between the agent (AUIA*STC*) and the agent secondary address spaces (AUIF*STC*, AUIL*STC*). Valid port numbers are 1 - 65535. Check with your network administrator for a list of ports available for this use.
Note:

- This keyword must be used in combination with ADS_SHM_ID.
- If you specify this keyword, you must add an //AUICONFG DD statement to the AUIF*STC* and AUIL*STC* address space JCLs. This DD statement should point to the same data set and member as the agent AUIA*STC* and AUIU*STC* JCLs to enable communication between all participating address spaces.

Syntax: ADS_LISTENER_PORT*(port_number)*
Example: ADS_LISTENER_PORT(16055)

APPLIANCE_SERVER

Required: Yes
Default: None
Description: The host name or IP address (in dotted decimal notation, for example: 1.2.3.4) of the IBM Guardium system to which the agent (AUIA*STC*) should connect.
Note: This parameter must be correctly configured to enable a connection to the IBM Guardium system. This value can contain up to 128 characters.
Syntax: APPLIANCE_SERVER*(hostname|IP_address)*
Example:

```
APPLIANCE_SERVER(wal-vm-guardium20)
APPLIANCE_SERVER(192.168.2.205)
```

APPLIANCE_SERVER_[1-5]

Required: No
Default: None
Description: Enables alternative host names or TCP/IP addresses to be used for multistream Guardium appliance destinations or failover recovery processing. Up to five alternative host names or TCP/IP addresses are supported.
To specify one or more entries, include this parameter with a numeric suffix from 1 - 5. Provide a unique host name or TCP/IP address for each entry.
Valid values are any valid host name or TCP/IP address.
Note:

- The use of this keyword does not eliminate the need for the APPLIANCE_SERVER keyword.
- The APPLIANCE_SERVER_LIST parameter designates how this parameter is used.
- If used in combination, this parameter overrides the APPLIANCE _SERVER_[MULTI_STREAM|FAILOVER|HOT_FAILOVER]_[1-5] parameter.

Syntax:

```
APPLIANCE_SERVER_n(hostname|IP_addr)
```

where *n* can be 1, 2, 3, 4, or 5.
Example:

```
APPLIANCE_SERVER_1(nwt-vm-guardium3)
APPLIANCE_SERVER_1(192.168.2.205)
```

APPLIANCE_SERVER_[MULTI_STREAM|FAILOVER|HOT_FAILOVER]_[1-5]

Required: No

Default: None
Description: The host name or IP address (in dotted decimal notation, for example: 1.2.3.4) of the IBM Guardium system for the IBM Guardium S-TAP for IMS agent to use to stream to multiple Guardium appliance destinations or for failover processing. This value can contain up to 128 characters.
Note:

- The use of this keyword does not eliminate the need for the APPLIANCE_SERVER keyword.
- If this parameter, or the APPLIANCE_SERVER_[1-5] parameter, is not detected at startup, then neither failover nor hot failover processing is activated.
- The APPLIANCE_SERVER_LIST parameter designates how this parameter is used.
- If used in combination, this parameter is overridden by the APPLIANCE_SERVER_[1-5] parameter.

Syntax:

```
APPLIANCE_SERVER_[MULTI_STREAM|FAILOVER|HOT_FAILOVER]_n(hostname|IP_address)
```

where *n* can be 1, 2, 3, 4, or 5.
Example:

```
APPLIANCE_SERVER_MULTI_STREAM_1(wal-vm-guardium20)
APPLIANCE_SERVER_FAILOVER_1(nwt-vm-guardium8)
APPLIANCE_SERVER_HOT_FAILOVER_1(wal-vm-guardium16)
APPLIANCE_SERVER_MULTI_STREAM_1(192.168.2.201)
APPLIANCE_SERVER_FAILOVER_1(192.168.2.202)
APPLIANCE_SERVER_HOT_FAILOVER_1(192.168.2.203)
```

APPLIANCE_SERVER_LIST(MULTI_STREAM|FAILOVER|HOT_FAILOVER)
Required: No
Default: FAILOVER
Description: Set APPLIANCE_SERVER_LIST to *MULTI_STREAM* for a Guardium appliance connection to be established for each server that is identified by the APPLIANCE_SERVER_MULTI_STREAM_n parameter.

- If a connection is lost, S-TAP audit events continue to transmit over the remaining appliance connection.
- Lost connections are retried at regular intervals that are determined by multiplying the APPLIANCE_CONNECT_RETRY_COUNT by the APPLIANCE_PING_RATE.

Set APPLIANCE_SERVER_LIST to *FAILOVER* for one Guardium appliance connection to be active at a time.

- If the connection to the primary appliance is lost, a failover action occurs, which results in an attempt to connect to the next available server. The next available server is identified by the APPLIANCE_SERVER_FAILOVER_n parameter. The agent attempts to connect to subsequent Guardium systems, beginning with APPLIANCE_SERVER_FAILOVER_1 and ending with APPLIANCE_SERVER_FAILOVER_5.
- After a failover action occurs, the connection to the primary server is retried at regular intervals that are determined by multiplying the APPLIANCE_CONNECT_RETRY_COUNT by the APPLIANCE_PING_RATE.

Set APPLIANCE_SERVER_LIST to *HOT_FAILOVER* to cause connection types for each connected Guardium appliance identified by the APPLIANCE_SERVER_HOT_FAILOVER_n parameter to be kept active by pings.

- You must specify the primary Guardium appliance by using the APPLIANCE_SERVER parameter.
- If the primary Guardium appliance becomes unavailable and failover occurs, *HOT_FAILOVER* maintains the activity of the primary appliance policy.

With any setting of APPLIANCE_SERVER_LIST, if all connections fail, and a spill file is specified (parameter OUTAGE_SPILLAREA_SIZE), events are buffered to the spill file until a connection becomes available. If no spill file is specified, and all connections are lost, data loss occurs.
The default is *FAILOVER*.

APPLIANCE_PORT
Required: No
Default: 16022
Valid ports: 16022 or 16023
Description: The IP port number of the IBM Guardium system to which the IBM Guardium S-TAP for IMS agent should connect. This parameter must be correctly configured to enable a connection to the IBM Guardium system. If port 16023 is used, encryption support is required for the connection to the appliance.
Note: Specifying this keyword and parameter designates the port on which the IBM Guardium system is listening to the S-TAP. The port is dedicated to the IP address of the appliance. Port 16022 or 16023 can also be in use on z/OS by another application.
Syntax: APPLIANCE_PORT*(port_number)*
Example: APPLIANCE_PORT(16022)

APPLIANCE_PING_RATE
Required: No
Default: 5
Description: Specifies the interval time between accesses to the IBM Guardium system to prevent timeout disconnections during idle periods. The value is in number of seconds.
Syntax: APPLIANCE_PING_RATE*(ping_interval)*
Example: APPLIANCE_PING_RATE(5)

APPLIANCE_NETWORK_REQUEST_TIMEOUT
Required: No
Default: 500
Description: Specifies a value in milliseconds of time to wait for the completion of a network communication request to send or receive. A value of 0 results in no timeout period. Range: 0 or 500 - 12000.
Syntax: APPLIANCE_NETWORK_REQUEST_TIMEOUT*(milliseconds)*
Example: APPLIANCE_NETWORK_REQUEST_TIMEOUT(500)

AUIU_EXCLUDE_LPAR
Required: No
Default: None
Description: Specifies a list of LPAR names (one to eight characters) in a SYSPLEX environment where the Common Storage Management Utility (AUIU*STC*) should not be scheduled. Multiple AUIU_EXCLUDE_LPAR statements can be specified to allow for LPAR name strings that are longer than 53 bytes.
Note: Use this keyword with caution. DLI calls run on the excluded LPARS are not audited.
With the exception of the LPAR where the agent resides, all LPARS can be excluded by using the option *ALL in place of an LPAR name.
Syntax: AUIU_EXCLUDE_LPAR(*list_of_lpars*)

Example: AUIU_EXCLUDE_LPAR(RS21,MYLPAR,YOURLPAR) or AUIU_EXCLUDE_LPAR(*ALL)

AUIU_PROC_NAME

Required: No

Default: AUIU*STC*

Description: Specifies the PROCLIB member name that contains the Common Storage Management Utility JCL. This JCL is supplied as member name AUIU*STC* in the sample library (AUISAMP). If multiple agents are used within a sysplex, each agent requires a separate JCL for each AUIU*STC* address space.

Syntax: AUIU_PROC_NAME*(auiu_mbr_name)*

Example: AUIU_PROC_NAME(AUIUV1013)

DISPLAY_IMSMSG_DLIB(Y|N)

Required: No

Default: N

Description: Controls the output of informational messages AUIJ255I, AUIJ256I, AUIJ257I, and AUIJ258I in the AUILOG output DD of the AUIA*STC* agent address space. These messages are generated from data that is produced by the IMS DLI/DB batch jobs, and is passed to the agent from the DLIB z/OS log stream.

The default setting, *N*, prevents these messages from being written to the AUILOG DD.

Specify *Y* for these messages to be written to the AUILOG DD.

Syntax: DISPLAY_IMSMSG_DLIB*(Y|N)*

Example: DISPLAY_IMSMSG_DLIB(Y)

DISPLAY_IMSMSG_DLIO(Y|N)

Required: No

Default: N

Description: Controls the output of informational messages AUIJ255I, AUIJ256I, AUIJ257I, and AUIJ258I in the AUILOG output DD of the AUIA*STC* agent address space. These messages are generated from data that is produced by the IMS Control Region and passed to the agent from the DLIO z/OS log stream.

The default setting, *N*, prevents these messages from being written to the AUILOG DD.

Specify *Y* for these messages to be written to the AUILOG DD.

Syntax: DISPLAY_IMSMSG_DLIO*(Y|N)*

Example: DISPLAY_IMSMSG_DLIO(Y)

DLIFREQ

Required: No

Default: 100K

Description: Enables you to customize the number of DLI calls that are sent to the Guardium appliance before message AUIJ012I (providing a count of the number of events sent to appliance) is issued.

The count can be represented in thousands (K) or millions (M). Valid values are 10K – 999K and 1 – 10M.

Syntax: DLIFREQ*(100K)*

Example: DLIFREQ(100K)

FORCE_LOG_LIMITED

Required: No

Default: N

Description: Enables you to force limited audit logging by removing sensitive information (such as IMS segment data and concatenated key values) from data that is sent to the Guardium appliance by the S-TAP.

Specify *Y* to restrict sensitive data from being sent to the Guardium appliance.

Syntax: FORCE_LOG_LIMITED*(Y|N)*

Example: FORCE_LOG_LIMITED(N)

IMSL_AUDIT_LEVELS

Required: No

Default: ALL

Description: Specifies the events to be audited from those that are found using the IMS Archive Log task (AUIL*STC*) for each IMS instance under control of this agent. A specification other than `ALL` limits auditing to the events you specify.

For example, if you specify `USERS`, then all audited IMS instances under the agent report user signons and signoffs. If you specify `ALL`, you can use the Guardium interface to specify further limitations on what is audited for each audited IMS subsystem.

Table 1. IMSL_AUDIT_LEVELS audit parameters and events.

Parameter	Audited event
ALL	All events are audited (default)
CTL_STRT	IMS control region stops and starts
USERS	User signon and signoff
DBOPN	Database opens and closes
DB_PSB	DBDDUMP, DB/PSB START/STOP/LOCK/UNLOCK

Syntax: IMSL_AUDIT_LEVELS*(ALL|CTL_STRT|USERS|DBOPN|DB_PSB)*

Example: IMSL_AUDIT_LEVELS(ALL)

IMSL_CYCLE_INTERVAL

Required: No

Default: 15

Description: Specifies the frequency (in minutes) that the IMS Archive Log task (AUIL*STC*) checks the RECON data sets for new IMS SLDS (System Log Data Sets) to process. This value should correspond to the frequency at which IMS generates SLDS data sets during a normal workload. For example, if IMS SLDS are produced every 20 minutes, the IMSL_CYCLE_INTERVAL should be set to 20. A value of 0 (zero) can be specified to instruct the agent not start the AUIL*STC* task for any IMS subsystem that the agent controls. Valid parameters are 0 – 1440.

Syntax: IMSL_CYCLE_INTERVAL*(time_in_minutes)*

Example: IMSL_CYCLE_INTERVAL(45)

IMSL_ID_PREFIX

Required: No
Default: None
Description: Allows the partial customization of the 8-byte ID that is used when starting the AUILSTC task.
When this keyword is not used, the string *AAAAAAAA* is used for the first AUILSTC task to be started. Subsequent started AUILSTC tasks cause the ALPHA string to be incrementally increased by one character until the value of *ZZZZZZZZ* is reached. When *ZZZZZZZZ* is reached, the string is reset to *AAAAAAAA* when the agent (AUIASTC) is stopped and restarted.
When this keyword is used, the specified prefix (up to 6 bytes) is used, while the remaining two to seven characters are incrementally increased in the manner previously described. This enables a constant value (the specified prefix) to be used, alongside a wildcard character, when you are defining the ID to the TCP/IP security package to permit access to TCP/IP ports.
Note: The first character of the keyword must be an alphabetic character.
Syntax: IMSL_ID_PREFIX*(your_prefix)*
Example: IMSL_ID_PREFIX(MYPFX)
The example IMSL_ID_PREFIX(MYPFX) results in a generated AUILSTC ID of *MYPFXAAA -- MYPFXZZZ*.

IMSL_PROC_NAME
Required: No
Default: AUIL*STC*
Description: Specifies the PROCLIB member name that contains the IMS Archive Log JCL. This JCL is supplied as member name AUIL*STC* in the sample library (AUISAMP). If multiple agents are used within a sysplex, each agent requires a separate JCL for each AUIL*STC* address space.
Syntax: IMSL_PROC_NAME*(auil_mbr_name)*
Example: IMSL_PROC_NAME(AUILV1013)

IMSL_SLDS_SRCH
Required: No
Default: 30
Description: This keyword can be used to limit the number of days within which the IMS log reader (AUILxxxx) will search for IMS system log data sets (SLDS) to process.

- If an IMS checkpoint does not exist for the SLDS reader, AUILxxxx will search for IMS SLDS that were created on the current day and for *x* days prior to the current day (where *x* is the value that you set for this parameter).
- If an IMS checkpoint that is set for the SLDS reader exceeds the number of days between the current day and the value that you set for this parameter, then the IMS checkpoint will be used as the starting point for IMS SLDS to be read and processed.
- If you set a value of *0* (zero) for this parameter, then only the current day's IMS SLDS will be processed. Also, IMS SLDS that were migrated from a hierarchical storage manager product will not be recalled for processing.
  Note: If you set a value of *0* (zero) for this parameter, AUILxxxx processing will omit any IMS SLDS that were created on the previous day. This can cause data to be missed if, for example, the AUILxxxx task is run at 12:05 AM. IMS SLDS that were created prior to midnight will not be recognized as being within the current day, and thus will not be processed.

Syntax: IMSL_SLDS_SRCH*(number_of_days)*
Example: IMSL_SLDS_SRCH(15)

LOG_FILTER(I/E)
Required: No
Default: I (include)
Description: Specifies whether to include or exclude messages that have been specified by the LOG_FILTER_MSG_ID parameter.

- The default value, `I`, allows only the specified message IDs to be included in the AUILOG output stream. Message IDs that are not specified by the LOG_FILTER_MSG_ID(messages) parameter will be suppressed. The default value should be used unless there is a specific business need to suppress messages.
- The optional value, `E`, suppresses the specified message IDs from the AUILOG output stream.
  Tip: The `E` value should only be used if the LOG_FILTER_MSG_ID keyword has been customized to suppress specific messages. Do not use the optional value (E) in conjunction with LOG_FILTER_MSG_ID(*) unless you want to prevent all messages from being written to the AUILOG output stream. Suppressing all messages is not recommended.

Syntax: LOG_FILTER*(include/exclude)*
Example: LOG_FILTER(E)

LOG_FILTER_MSG_ID(messages)
Required: No
Default: * (all messages)
Description: Can be used in conjunction with the LOG_FILTER(I/E) parameter to suppress specific messages from being written to the AUILOG output stream.
Tip: The LOG_FILTER_MSG_ID(*) default value should only be used with the LOG_FILTER(I) default value. Do not specify LOG_FILTER(E) in conjunction with LOG_FILTER_MSG_ID(*) unless you want to prevent all messages from being written to the AUILOG output stream. Suppressing all messages is not recommended.
Syntax: LOG_FILTER_MSG_ID*(id1,id2,id3...)*
Example: LOG_FILTER_MSG_ID(AUIZ014W)

LOG_PORT_SCAN_START
Required: No
Default: 41500
Description: Specifies the first communications port number to be checked for availability to be used for internal message logging communications. Use this keyword if environmental conditions dictate that a sequential scan and test of ports from port numbers 41500 - 65535 should not be performed. You can override the starting port with a port of your choice. This keyword and parameter can be used with the LOG_PORT_SCAN_COUNT keyword to limit the ports that are scanned to a specific range.
Syntax: LOG_PORT_SCAN_START*(port_number)*
Example: LOG_PORT_SCAN_START(41500)

LOG_PORT_SCAN_COUNT
Required: No
Default: 10
Description: This keyword can be used in conjunction with the LOG_PORT_SCAN_START keyword to limit number of the ports that are scanned and tested for availability. The integer specified (1 - 65535) represents the number of ports that should be scanned. If the port number specified by the LOG_PORT_SCAN_START value plus the LOG_PORT_SCAN_COUNT value exceeds 65535, the scan terminates at port 65535.
Syntax: LOG_PORT_SCAN_COUNT*(number_of_ports)*
Example: LOG_PORT_SCAN_COUNT(1000)

LOG_STREAM_DLIB
Required: Yes
Default: None

Description: This required keyword is used to specify the z/OS System Logger log stream to stream audited events from DLI DBB batch jobs. The value should be the BATCH_LOGSTREAM_NAME value specified as the DEFINE LOGSTREAM NAME parameter of the AUILSTR2 or AUILSTR3 JCLs.
Syntax: LOG_STREAM_DLIB*(log_stream_name)*
Example: LOG_STREAM_DLIB(AUI_BATCH_LOG_STREAM)

LOG_STREAM_DLIO

Required: Yes
Default: None
Description: This required keyword is used to specify the z/OS System Logger log stream to be used to stream audited events from IMS Control Regions. The value should be the ONLINE_LOGSTREAM_NAME value specified as the DEFINE_LOGSTREAM_NAME parameter of the AUILSTR2 or AUILSTR3 JCLs.
Syntax: LOG_STREAM_DLIO*(log_stream_name)*
Example: LOG_STREAM_DLIO(AUI_ONLINE_LOG_STREAM)

LOOPBACK_ADDRESS

Required: No
Default: LOCALHOST
Description: Specifies the loopback host or IP address that is used for communications between the agent and the agent secondary address spaces. For most network configurations, the default value of `LOCALHOST` can be used. If `LOCALHOST` cannot be resolved on your system, consult your network specialist for the correct loopback mnemonic or IP address to be used.
Syntax: LOOPBACK_ADDRESS*(hostname|IP_address)*
Example: LOOPBACK_ADDRESS(LOCALHOST)

LPAR_MONITOR_INTERVAL

Required: No
Default: 5
Description: Specifies the frequency (in minutes) for the agent to request a list of LPARs that are active within the SYSPLEX. Schedule the Common Storage Management Utility (AUIU*STC*) tasks on any LPAR coming online to the SYSPLEX. Valid parameters are integers between 1 and 60.
Syntax: LPAR_MONITOR_INTERVAL*(minutes)*
Example: LPAR_MONITOR_INTERVAL(5)

MESSAGE_LOG_LEVEL

Required: No
Default: I
Description: Controls the amount of output log information that is generated by the agent.

Table 2. Message severity codes and descriptions.

Message severity code	Description
I	Includes all log messages
W	Includes all log messages with a warning severity or higher
E	Includes all log messages with an error severity or higher
O	Instructs the agent not to log error messages
S	Includes all log messages with a severe error code

Syntax: MESSAGE_LOG_LEVEL*(I|W|E|O|S)*
Example: MESSAGE_LOG_LEVEL(I)

OUTAGE_SPILL_AREA_SIZE

Required: No
Default: 0
Description: Determines the maximum amount of memory in megabytes to be allocated for the retention of audit data in the event of a IBM Guardium system connection outage. A value of `0`, or the absence of this keyword, disables spill area support. The maximum value permitted as a parameter is 1024.
Syntax: OUTAGE_SPILL_AREA_SIZE*(memory_size)*
Example: OUTAGE_SPILL_AREA_SIZE(15)

POLICY_READ_INTERVAL

Required: No
Default: 5
Description: Determines the frequency in seconds that the connection to the IBM Guardium system checks for changes to the installed policies that are used to determine audited event collection.
Syntax: POLICY_READ_INTERVAL*(time_in_seconds)*
Example: POLICY_READ_INTERVAL(5)

STAP_STREAM_EVENTS

Required: No
Default: Y
Description: Specifies whether events will be streamed to the IBM Guardium system. The default value, *Y*, enables streaming. Specify *N* to disable streaming and enable Simulation mode.
Syntax: STAP_STREAM_EVENTS*(Y|N)*
Example: STAP_STREAM_EVENTS(Y)

PREFER_IPV4_STACK

Required: No

Default: N

Description: If set to Y, this parameter causes a request to be issued to the Domain Name Server (DNS) for an IPV4 address for the hostname that is specified in the APPLIANCE_SERVER parameter:

- The DNS lookup request for an IPV4 address is attempted. If an IPV4 address is defined for the hostname, the DNS will respond with the value that will be used to connect to the Guardium appliance.
- If only an IPV6 address is defined at the DNS, then the DNS will respond with the IPV6 address that will be used to connect to the Guardium appliance.
- If both IPV4 and IPV6 addresses are defined at the Guardium appliance, the DNS will respond with both addresses, and the IPV4 address will be used to connect to the appliance.

If this parameter is set to N or omitted from configuration, a request for an IPV6 address is issued to the DNS for the hostname that is specified by the APPLIANCE_SERVER parameter:

- The DNS lookup request for an IPV6 address is attempted. If an IPV6 address is defined for the hostname, the DNS will respond with the value that will be used to connect to the Guardium appliance.
- If only an IPV4 address is defined at the DNS, then the DNS will respond with the IPV4 address that will be used to connect to the Guardium appliance.
- If both IPV4 and IPV6 addresses are defined at the Guardium appliance, the DNS will respond with both addresses, and the IPV4 address will be used to connect to the appliance.

Note: Whether or not this parameter is used, if the address returned from the DNS is not valid for the hostname, it will result in failure to connect to the appliance, and the IBM Guardium S-TAP for IMS started task will terminate.

Syntax:

```
PREFER_IPV4_STACK(Y|N)
```

Example:

```
PREFER_IVP4_STACK(Y)
```

SMF_AUDIT_LEVELS

Required: No

Default: ALL

Description: Specifies which events to audit of those found using the SMF task (AUIF*STC*). A specification other than `ALL` limits the events to be audited to the events you specify. For example, if `DELETE` is specified, then all audited IMS instances under the agent would only be capable of reporting data set `DELETE` events. If `ALL` is specified, you can further limits what is audited for each audited IMS subsystem, using the user interface.

Table 3. SMF_AUDIT_LEVELS audit parameters and events

Parameter	Audited event
ALL	All events are audited (default)
UPDATE	Data sets opened with UPDATE access
DELETE	Data sets deleted
READ	Data sets opened with READ access
CREATE	Data sets created
ALTER	Data sets opened with ALTER access
RACF®	RACF violations on data sets

Syntax: SMF_AUDIT_LEVELS*(ALL|UPDATE|DELETE|READ|CREATE|ALTER|RACF)*

Example: SMF_AUDIT_LEVELS(ALL)

SMF_CYCLE_INTERVAL

Required: No

Default: 300

Description: Specifies the frequency (in minutes) that the SMF task (AUIFSTC) checks the z/OS catalog for new data sets, which meet the specified data set masks, using the SMF_DSN_MASK keyword. This value should correspond to the frequency at which your z/OS system swaps SMF logging VSAM files (sometimes known as SMF MANX|MANY) during a normal workday. For example, if the SMF logging files are swapped every 8 hours, the SMF_CYCLE_INTERVAL should be set to `480` (8 hours * 60 minutes). A value of zero can be specified to indicate that the agent should not start the AUIF*STC* task and SMF auditing should not be performed. Valid parameters are 0 – 1440.

Syntax: SMF_CYCLE_INTERVAL*(time_in_minutes)*

Example: SMF_CYCLE_INTERVAL(45)

SMF_DSN_MASK_[1-10]

Required: Yes

Default: None

Description: At least one instance of this keyword is required (SMF_DSN_MASK_1). This keyword provides a data set mask used to query the z/OS catalog for sequential format data sets containing SMF data offloaded from the SMF log-files (MANX|MANY) using the IFASMFDP program. These sequential files can be the original files created when offloading the MANX|MANY files, or a copy of these sequential files created by customizing and running AUISMFDF and AUISMFDP jobs located in the product sample data set. In most environments, only one SMF_DSN_MASK would be specified, but up to 10 are allowed.

Table 4. Masking character rules

Character	Rule
%	Indicates that only one alphanumeric or national character can occupy that position
%%%	Indicates that more than one character can be substituted, with the number of substitution characters being equal to the number of percent signs specified.

Example 1: specifying a GDG data set in the mask: If the AUISMFDP job has been customized to produce a GDG data set as the SORTOUT DD output data sets, you can choose to specify the fully qualified GDG base name in the mask for system name field. For example, A.B.C. IBM Guardium S-TAP for IMS uses catalog services to determine the names of all cataloged GDG entries under this name, for example:

- A.B.C.G0001V00
- A.B.C.G0002V00
- A.B.C.G0003V00

Example 2: specifying a data set name explicitly: Provide the generation and version values as a mask. For example, A.B.C.G%%%%V%%. IBM Guardium S-TAP for IMS uses catalog services to determine the names of all cataloged data sets that match this mask, for example:

- A.B.C.G0021V00
- A.B.C.G0022V00
- A.B.C.G0023V00

Example 3: specifying a DSN using a DATE/TIME naming convention: If you have customized the AUISMFDP job to produce a data set name that contains date and time values as qualifiers within the data set name as the SORTOUT DD output data sets, you can specify the data set name using a string of percent signs within the date and time qualifier names. For example: HLQ.D%%%%%%.T%%%%%%.SMFDATA. IBM Guardium S-TAP for IMS uses catalog services to determine the names of all cataloged data sets matching the mask, for example:

- HLQ.D091122.T131000.SMFDATA
- HLQ.D091123.T131100.SMFDATA
- HLQ.D091124.T131200.SMFDATA

Note: The percent (%) wildcard character should only be specified for the numeric characters of the generation and version node of GDG data sets, or as the numeric characters of date or time nodes of the SMF dataset.
Syntax: SMF_DSN_MASK_1*(SMF.DUMP.DSN)*
Example:

```
SMF_DSN_MASK_1(AUI.SMF.DUMP.COPY)
SMF_DSN_MASK_2(AUI.SMF.DUMP.GDG.G%%%%V%%)
SMF_DSN_MASK_3(AUI.SMF.D%%%%%%.T%%%%%%.COPY)
```

SMF_EVENT_EXPIRY
Required: No
Default: 5
Description: Specifies the number of days that incomplete SMF events should be retained in the SMF spill file. Incomplete SMF events are audited events that have not yet received the associated SMF Type 30 record, which indicates that the step/job is complete, and contains information that is needed to complete the reporting of the event. When an event exceeds the expiration date, it is flagged as incomplete, sent to the IBM Guardium system, and removed from the SMF spill file. The valid range is 1 to 180 days.
Syntax: SMF_EVENT_EXPIRY*(days)*
Example: SMF_EVENT_EXPIRY(5)

SMF_PROC_NAME
Required: No
Default: AUIFSTC
Description: Specifies the PROCLIB member name that contains the SMF secondary address space JCL. This JCL is supplied as member name AUIF*STC* in the sample library (AUISAMP). If multiple agents are used within a sysplex, each agent requires a separate JCL for each AUIF*STC* address space.
Syntax: SMF_PROC_NAME*(auif_mbr_name)*\
Example: SMF_PROC_NAME(AUIFV91)

SMF_SELF_AUDIT
Required: No
Default: N
Description: Indicates whether to audit the accesses of IMS data sets that are used by the product to determine the names of IMS artifacts to be audited. Examples of IMS data sets that can be accessed include RECON data sets and IMS archived logs (SLDS). A value of `N` indicates that these accesses should not be audited. A value of `Y` indicates that these data sets should be considered for auditing.
Syntax: SMF_SELF_AUDIT*(N|Y)*
Example: SMF_SELF_AUDIT(N)

SMF_SPILL_FILE
Required: Yes
Default: None
Description: Specifies the DSN of a sequential format fixed block data set with a LRECL of 300. This data set is used to store incomplete audited SMF events. Incomplete audited SMF events are events triggered by SMF records that have yet to encounter an SMF Type 30 record, indicating the step or job has completed. The AUIFUSPL member of the SAUISAMP data set provides an example of the allocation specifications for this data set.
Syntax: SMF_SPILL_FILE*(dsn)*
Example: SMF_SPILL_FILE(AUI.V1013.SPILL)

TCPIP_BUFFER_SIZE
Required: No
Default: 32768
Description: Specifies the size of an internal buffer that is used to hold audited events in preparation of the TCP/IP send to the IBM Guardium system, and specifies the size of the TCP/IP buffer. In most environments, the size of this buffer should not be changed
Syntax: TCPIP_BUFFER_SIZE*(buffer_size)*
Example: TCPIP_BUFFER_SIZE(32768)

TRACE_CONFIG
Required: No
Default: ON
Description: TRACE_CONFIG(ON) enables IBM Guardium S-TAP for IMS configuration values to display by default at agent startup. You can optionally use this keyword to disable the IBM Guardium S-TAP for IMS configuration value display. To prevent the displayed report of agent configuration parameters during agent startup, specify TRACE_CONFIG(OFF).
Syntax: TRACE_CONFIG*(ON|OFF)*
Example: TRACE_CONFIG(OFF)

WTO_MSG
Required: No
Default: None
Description: Allows a user to request that specific informational, warning, or error messages written to the AUILOG DD statement of the agent (AUIA*STC*) or agent secondary address spaces (AUIF*STC*, AUIL*STC* or AUIU*STC*) also be written to the Operator Console (WTO). This enables these messages to be recognized by an automated operations tool, or provides higher operator visibility for these messages and allows appropriate action to be taken. Each message requires a separate keyword, and each keyword must be specified on a separate line.
Syntax: WTO_MSG*(msgnumber)*
Example:

```
WTO_MSG(AUIJ011I)
WTO_MSG(AUIL607W)
WTO_MSG(AUIY006E)
```

XML_ECHO_AUILOG(Y|N)
Required: No
Default: N
Description: Indicates that when an audit policy is installed on a IBM Guardium system appliance, its corresponding XML is to be echoed to the AUILOG DD. If there is more than one policy installed on the agent, the XML of each policy is echoed. If all installed policies are subsequently uninstalled, then the echoed XML reflects that there are no installed policies. For more information about echoed XML statements, see XML statement definitions.
Syntax: XML_ECHO_AUILOG(Y|N)
Example: XML_ECHO_AUILOG(Y)

XML_ECHO_DATASET(Data_Set_Name[,Cylinders])
Required: No
Default: None
Description:

Indicates that when the IBM Guardium system installs an audit policy, its corresponding XML is echoed to a data set (specified by the data set name value in this parameter). If there is more than one policy installed on the agent, the XML of each is echoed. If all installed policies are subsequently uninstalled, then the echoed XML reflects that there are no installed policies. The XML will not be echoed when the installed policy is already active, is being reinstalled, and there have been no changes to the policy.

If *Data_Set_Name* is intended to be a Generation Data Group (GDG), then it must be set as the GDG base name. The agent checks the system catalog to determine whether *Data_Set_Name* exists and whether or not it is a GDG base name.

Data_Set_Name can contain z/OS system symbols such as &SYSNAME. To determine the names of the system symbols that are currently defined to the system, issue the DISPLAY SYMBOLS command to the system console.

If *Data_Set_Name* does not exist, and there is no GDG base defined in this name, the agent allocates the data set as non-GDG. If *Data_Set_Name* is a regular physical sequential data set (non-GDG based) and does exist, the agent allocates space for the *Cylinders* keyword when the agent is restarted.

Cylinders defaults to 1 and can range from 1 – 10.
Syntax: XML_ECHO_DATASET*(&Data_Set_Name[,Cylinders])*
Example: XML_ECHO_DATASET(AUIAGENT.ECHO.XML.GDG.BASE,2)

ZIIP_AGENT_DLI
Required: No
Default: N
Description: Indicates that the following agent processes should be zIIP capable: agent reads of audited events from the z/OS System Logger log streams, formatting of these events into protobuf style messages, and sending of these messages to the IBM Guardium system using TCP/IP.
Note: Use of the zIIP depends on the presence of a zIIP on the LPAR where the agent is running, as well as use of the Workload Management Service Policies. For more information about zIIP, see the topic on Customizing IMS to use a System z® Integrated Information Processor (zIIP).
Syntax: ZIIP_AGENT_DLI*(Y|N)*
Example: ZIIP_AGENT_DLI(Y)

Parent topic: Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent

Related reference

- Customizing IMS to use a System z Integrated Information Processor (zIIP)

Agent configuration

The IP addresses of the IBM Guardium system appliances are specified using the SAUISAMP data set AUICONFG member using the APPLIANCE_SERVER and APPLIANCE_SERVER_FAILOVER_[1-5] keywords.

See Providing Guardium system failover for more information.
Parent topic: Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent

Customizing the agent JCL

The SAUISAMP member AUIA*STC* provides a sample JCL that can be used for the agent started task. This topic describes how to customize the JCL.

Before you begin

In environments where multiple agents connect to a common IBM Guardium system or appliance, the z/OS agent started task names (AUIA*STC*, AUIL*STC*, AUIF*STC*) must be unique. Unique started task names enable the IBM Guardium S-TAP for IMS policies that are pushed from the IBM Guardium system to be attributed to, and monitored by, the correct z/OS agent.

Procedure

1. Edit SAUISAMP members AUIA*STC*, AUIF*STC*, AUIL*STC* and AUIU*STC* by running the ISPF edit macro.
   See Planning your configuration and customizing your environment for more details.
2. Modify the CFG=AUI.V100.AGTCFG(AUICONFG) in AUIA*STC* to specify the location of the customized configuration data set for the agent created in the previous section.
3. Optional: You can rename the AUIA*STC* member to any character name that is valid for started tasks in your environment.
4. Optional: You can rename the AUIF*STC*, AUIL*STC*, and AUIU*STC*. AUIF*STC*, AUIL*STC*, and AUIU*STC* names should match the values of the IMSL_PROC_NAME, SMF_PROC_NAME, and AUIU_PROC_NAME keywords that you supply in the configuration file.
5. Copy the AUIA*STC*, AUIF*STC*, AUIL*STC* and AUIU*STC* members to the PROCLIB for the site.
   Contact the z/OS systems programmer to determine the location of the PROCLIB.
   Note: APF authorization of the AUILOAD file is required for each of these members before they are started.

Parent topic: Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent

Starting and stopping the agent

Start the agent by issuing the command /S AUIASTC from the SDSF command line. The primary agent address space starts the AUIF*STC* address spaces. One or more instances of AUIL*STC* might also be started, depending on the list of active collections.

Stop the agent by issuing the command /STOP AUIASTC, or /MODIFY AUIASTC,STOP, from the SDSF command line. The primary agent address space then stops all the secondary address spaces that are online, and shuts down. Depending on the load, and the activity in the other secondary address spaces, the shut down process can take time. Monitor the AUILOG DD of the primary address space AUIA*STC* for informational messages on the status of the secondary address spaces.

Parent topic: Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent

Agent security considerations

The user ID of the agent started tasks (the primary and the secondary started tasks) should have the necessary RACF® profiles for reading the configuration member contents.

Important: Contact your system administrator to ensure that localhost is resolving to 127.0.0.1 (loopback address). The TCP/IP communication between the agent and the secondary address spaces relies on this resolution. If this is not possible at your site, use the *loop-back-address* element in the AUICONFG sample library member to avoid localhost resolution by specifying the loopback IP address directly, or by specifying an appropriate host name that resolves to the loopback address.
Parent topic: Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent

Modifying the frequency of AUIJ012I messages

You can modify how frequently the agent provides a count of DLI calls (from the default of every 10K DLI calls to a value of your choice, 10K – 999K, 1M – 10M.)

Use the agent parameter keyword DLIFREQ to modify the frequency of AUIJ012I messages, or issue the command /MODIFY AGENT,SET CONFIG DLIFREQ *aaaK* | *bbM*, from the SDSF command line.

Parent topic: Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent

Setting up an IMS environment for auditing

This section describes how to customize IMS environments to capture DLI calls, including customizing IMS catalogued procedures, coexisting with other DFSFLGX0 and DFSISVI0 exit routines, customizing IMS to use a zIIP, copying common load modules from SAUILOAD to SAUIIMOD, and the security considerations related to IMS processing.

- **Security considerations for IMS processing**
  IBM Guardium S-TAP for IMS does not impose any additional RACF® or other security restrictions on IMS assets during IMS processing. However, the IMS control region and any DLI/DBB batch jobs being executed, must have UPDATE authority to the z/OS system log streams you have defined for use by IBM Guardium S-TAP for IMS.
- **Customizing IMS environments to capture DLI calls**
  For IBM Guardium S-TAP for IMS to report on IMS database accesses, it needs to be sensitive to IMS DL/I calls. Use the following sections to establish proper set-up of the relationship between your IMS online and batch environments and IBM Guardium S-TAP for IMS.
- **Customizing IMS cataloged procedures**
  For IBM Guardium S-TAP for IMS to monitor DL/I calls from IMS online Transactions, BMPs and DLI/DBB batch jobs, the IMS Control region and DLI/DBB batch jobs require access to these IBM Guardium S-TAP for IMS programs.
- **Coexisting with other DFSFLGX0 and DFSISVI0 exit routines**
  IBM Guardium S-TAP for IMS provides product-specific DFSFLGX0 (IMS Logger) and DFSISVI0 (IMS Batch) exits to enable the product to report on IMS DL/I call activity. In some IMS environments, user requirements or third-party vendor products also require the use of these exits. IBM Guardium S-TAP for IMS can accommodate the use of multiple DFSFLGX0 and DFSISVI0 exit routines.
- **Defining LOGWRT exits**
  Use the EXITDEF parameter in the USER_EXITS section of the DFSDFxxx IMS PROCLIB member to define LOGWRT exits to be used by your IMS subsystem.
- **Customizing IMS to use a System z Integrated Information Processor (zIIP)**
  IBM Guardium S-TAP for IMS allows you to configure an IMS control region to prepare specific auditing functions for execution on a System z® Integrated Information Processor (zIIP). Execution on a zIIP is governed by the Workload Management software on your appliance, as well as the workload already assigned to the zIIP.
- **Copying common load modules from SAUILOAD to SAUIIMOD**
  After the initial SMP/E installation of IBM Guardium S-TAP for IMS, copy common load modules from the SAUILOAD to SAUIIMOD data set using the modules described in this topic.
- **Configuring APP_EVENT support**
  IBM Guardium S-TAP for IMS allows IMS DLI application programs to store user information on the IBM Guardium system. This enables your user data to be linked with DLI DB calls that are made from within the same application checkpoint, unit-of-work, or commit. APP_EVENT calls are linked to audited DLI calls by subsystem ID, application sequence number, and number of commits within a schedule. Follow these steps to install and configure a new IMS database, named AUIAPPEV, to be used for this purpose.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Security considerations for IMS processing

IBM Guardium S-TAP for IMS does not impose any additional RACF® or other security restrictions on IMS assets during IMS processing. However, the IMS control region and any DLI/DBB batch jobs being executed, must have UPDATE authority to the z/OS system log streams you have defined for use by IBM Guardium S-TAP for IMS.

Parent topic: Setting up an IMS environment for auditing

Customizing IMS environments to capture DLI calls

For IBM Guardium S-TAP for IMS to report on IMS database accesses, it needs to be sensitive to IMS DL/I calls. Use the following sections to establish proper set-up of the relationship between your IMS online and batch environments and IBM Guardium S-TAP for IMS.

Note: The IBM Guardium S-TAP for IMS programs that are used to communicate with your IMS environments are found in the SAUIIMOD data set, and are created during product installation.
Parent topic: Setting up an IMS environment for auditing

Customizing IMS cataloged procedures

For IBM Guardium S-TAP for IMS to monitor DL/I calls from IMS online Transactions, BMPs and DLI/DBB batch jobs, the IMS Control region and DLI/DBB batch jobs require access to these IBM Guardium S-TAP for IMS programs.

The IBM Guardium S-TAP for IMS programs that must be accessed reside in the SAUIIMOD installation data set. The preferred method of installing IBM Guardium S-TAP for IMS into your IMS environment is to copy the entire contents of the SAUIIMOD data set into your IMS RESLIB (IMS.SDFSRESL) data set.

If copying IBM Guardium S-TAP for IMS programs into your IMS RESLIB is not possible, then the SAUIIMOD data set must be included in your IMS control region JCL as the first data set of the STEPLIB DD concatenation. The SAUIIMOD data set must also be included as the first data set of the STEPLIB DD concatenation of the DLI batch cataloged procedure (DLIBATCH member of the IMS PROCLIB data set) and the DBB batch cataloged procedure (DBBBATCH member of the IMS PROCLIB data set).

Note:

- If the SAUIIMOD data set is included in any JCL, you must ensure that it is APF-authorized.
- IBM Guardium S-TAP for IMS provides and uses the DFSFLGX0 and DFSISIV0 IMS exits to establish communication with IMS services, however no customization of these exits is required.

Parent topic: Setting up an IMS environment for auditing

Coexisting with other DFSFLGX0 and DFSISVI0 exit routines

IBM Guardium S-TAP for IMS provides product-specific DFSFLGX0 (IMS Logger) and DFSISVI0 (IMS Batch) exits to enable the product to report on IMS DL/I call activity. In some IMS environments, user requirements or third-party vendor products also require the use of these exits. IBM Guardium S-TAP for IMS can accommodate the use of multiple DFSFLGX0 and DFSISVI0 exit routines.

Using IMS Tools Generic Exits

IMS Tools Generic Exits are a collection of components that provide common command and exit routine interfaces to support the operation of IMS tools in an IMS environment.

IBM Guardium S-TAP for IMS supports the protocols used by the IMS Tools Generic Exit product. You can define the IBM Guardium S-TAP for IMS copy of the DFSFLGX0 exit by either supplying IMS with a PROCLIB member using a BPE-style control statement, or by building a load module that contains the required information.

An example of the PROCLIB control statement follows:

```
EXITDEF(TYPE(LOGR) EXITNAME(AUIFLGX0) LOADLIB(AUI.SAUIIMOD))
```

See the IBM IMS Tools Generic Exit Reference Manual for Generic Logger Exit setup and usage.
Important: The IBM IMS Tools Generic Exit product does not support exit DFSISVI0.

Using IBM Guardium S-TAP for IMS exit cascading

For situations where the IBM IMS Tools Generic Exit is not available for use, IBM Guardium S-TAP for IMS provides a method of supporting two instances of the DFSFLGX0 and DFSISVI0 exits.

When loaded and run, the IBM Guardium S-TAP for IMS supplied program AUIFLGX0 (DFSFLGX0) and AUIISVI0 (DFSISIV0) determines from which DSN within the JOBLIB/STEPLIB concatenation it was loaded from. It then searches all subsequent DSNs within the JOBLIB/STEPLIB DD concatenation, looking for the next occurrence of the exit with the same name.

- If none are found, or it is determined that the IMS Tools Generic Exit product is involved in executing the exit, no cascading is done.
- If an exit is found, and it is determined that the exit found is in fact another instance of the IBM Guardium S-TAP for IMS exit (as could happen if the SAUIIMOD data set was specified multiple times in the JOBLIB/STEPLIB concatenation), the search will continue with the remainder of the DSNs in the concatenation.
- If a non-IBM Guardium S-TAP for IMS Exit is found, this new exit is loaded, and called with R13 pointing to the save area supplied by IMS. A new 512 byte user work area, obtained specifically for this exit instance, is then pointed to by the SXPLAWRK field of the IMS Standard User Exit Parameter List (DFSSXPL). This 512 byte work area is obtained when the first (or INIT) call is done; the work area address (in the SXLPAWRK field) and work area content are maintained for all subsequent calls.

Exit cascading restrictions

Note: These restrictions only apply when using the exit cascading feature, and not when using the IBM IMS Tools Generic Exit product.
The IBM Guardium S-TAP for IMS Exit (AUIFLGX0 or AUIISVI0) must be first in the JOBLIB/STEPLIB concatenation, unless the exit that exists in a prior DSN also has a method of cascading calls to other exits, and is capable of providing an IMS formatted area in R13 and the address of a unique, persistent 512 byte work area in the SXPLAWRK parameter list field to the AUIFLGX0 or AUIISVI0 program.

In a non-APF-authorized environment, such as when executing program DFSULTR0 or an IMS DLI/DBB batch program, the exit load module to be cascaded to must have an ALIAS, and the ALIAS must be appropriately either DFSFLGX0 or DFSISVI0, if the target exit module has the RENT or REUS attribute on.

Parent topic: Setting up an IMS environment for auditing

Defining LOGWRT exits

Use the EXITDEF parameter in the USER_EXITS section of the DFSDFxxx IMS PROCLIB member to define LOGWRT exits to be used by your IMS subsystem.

You must specify the exit name AUIFLGX0 in the list of LOGWRT exits to be used. This disables the cascading feature, which prevents other LOGWRT exits in the STEPLIB from being unintentionally invoked. You must include the SAUIIMOD load library in the IMS Control Region STEPLIB concatenation.

Example:

```
<SECTION=USER_EXITS>
EXITDEF=(TYPE=LOGWRT,EXITS=(AUIFLGX0))
```

Parent topic: Setting up an IMS environment for auditing

Customizing IMS to use a System z Integrated Information Processor (zIIP)

IBM Guardium S-TAP for IMS allows you to configure an IMS control region to prepare specific auditing functions for execution on a System z® Integrated Information Processor (zIIP). Execution on a zIIP is governed by the Workload Management software on your appliance, as well as the workload already assigned to the zIIP.

To use this feature, the LPAR on which the IMS Control region executes must have a zIIP installed. The IMS Control Region should also make use of the z/OS Workload Manager product. For more information on using z/OS Workload Manager with the IMS Control Region, see the *Workload Manager and IMS* section of the *IBM IMS System Administration* manual.

The following processes can be scheduled on a zIIP:

- Calling of the compiled filter to determine if the DLI event is to be audited, and if the segment concatenated key or segment data should be sent to the Guardium appliance.
- Movement of the audited DLI calls to a storage buffer used to hold audited data until a write to the z/OS System Logger log-stream can be executed
- Calling of the z/OS System Logger IXGWRITE, which moves the audited data from the buffer to the log-stream when the buffer fills, or a flush of the buffer is scheduled

To indicate that the IMS Control region should attempt to schedule these processes on the zIIP, a //AUIZIIP DD DUMMY DD statement should be added to the IMS Control Region JCL. When detected, the audit code produces the informational message AUII055I, indicating that zIIP processing will be attempted.

Warning messages AUII042W and AUII043W are issued if zIIP processing is requested when a zIIP is not available, and when IMS is not using Workload Manager. Error message AUII044E indicates that the request was rejected. In all instances where the attempt to use the zIIP has failed, audit processing continues without attempting to execute the audit code on the zIIP.

Parent topic: Setting up an IMS environment for auditing

Related reference

- Customizing the agent by using agent parameter keywords

Copying common load modules from SAUILOAD to SAUIIMOD

After the initial SMP/E installation of IBM Guardium S-TAP for IMS, copy common load modules from the SAUILOAD to SAUIIMOD data set using the modules described in this topic.

AUI$NAP
: Module used to trace data
Provided in the SAUILOAD data set
Also needed in the SAUIIMOD data set

AUICPMOD
: An SAUISMAP member
Performs a copy of the AUI$NAP module from the SAUILOAD to the SAUIIMOD data set
Should be customized and submitted after the initial SMP/E installation

Parent topic: Setting up an IMS environment for auditing

Configuring APP_EVENT support

IBM Guardium S-TAP for IMS allows IMS DLI application programs to store user information on the IBM Guardium system. This enables your user data to be linked with DLI DB calls that are made from within the same application checkpoint, unit-of-work, or commit. APP_EVENT calls are linked to audited DLI calls by subsystem ID, application sequence number, and number of commits within a schedule. Follow these steps to install and configure a new IMS database, named AUIAPPEV, to be used for this purpose.

Procedure

1. Perform a Database Descriptor Generator (DBD gen) for the AUIAPPEV database.
   An example of the DBD source to use is in member AUIAPPEV of the SAUISAMP data set.
2. Create a database data set for the AUIAPPEV database.
3. If appropriate for your site, register the DB and DDN to DBRC, specifying NOREOV if possible.
4. If appropriate for your site, create a dynamic allocation (MDA) member for the database data set.
5. Modify application program PSBs to include a PCB for the AUIAPPEV database.
   Use a PROCOPT of *G* and a KEYLENGTH of *0*.
6. If the APP_EVENT feature is to be used by an IMS Online system, perform an ACBGEN for DBD member AUIAPPEV and the modified PSBs.
7. Modify application programs to send APP_EVENT information using the AUIAPPEV PCB:
   a. In the 2000 byte I/O area, modify the application programs to include the information that you want to be sent to the appliance.
   b. Perform a DLI GET call by using the AUIAPPEV PCB.
      A DLI status code of blanks will be returned.

- **APP_EVENT examples**
  Examples of the AUIAPPEV database, a PSB with DBPCB for the AUIAPPEV database included, the Assembler language of an IMS DLI call, and a C program are provided here. These code samples are for example purposes only. There is no guarantee of the reliability, serviceability, or function of these programming examples.

Parent topic: Setting up an IMS environment for auditing

APP_EVENT examples

Examples of the AUIAPPEV database, a PSB with DBPCB for the AUIAPPEV database included, the Assembler language of an IMS DLI call, and a C program are provided here. These code samples are for example purposes only. There is no guarantee of the reliability, serviceability, or function of these programming examples.

AUIAPPEV database

The AUIAPPEV database is used to support the transmittal of environmental information from an application program to the Guardium appliance. The following is an example:

```
DBD                    NAME=AUIAPPEV,ACCESS=(HDAM,OSAM),RMNAME=(DFSHDC40,10,20)
DATASET                DD1=AUIAPPEV,SIZE=2048
SEGM       NAME=ROOT,PARENT=0,BYTES=2000
DBDGEN
FINISH
END
```

PSB with DBPCB for the AUIAPPEV database included

The following is an example of a PSB with DBPCB for the AUIAPPEV database included:

```
PCB             TYPE=DB,PROCOPT=A,KEYLEN=4,DBDNAME=AUEVOL01,  PCBNAME=ODBPCB1
SENSEG          NAME=ROOT,PARENT=0
PCB             TYPE=DB,PROCOPT=G,KEYLEN=0,DBDNAME=AUIAPPEV,  PCBNAME=APPEV01
SENSEG          NAME=ROOT,PARENT=0
PSBGEN          LANG=ASSEM,CMPAT=YES,PSBNAME=AUIPSBAV
END
```

Assembler language of an IMS DLI call

The following is an example in the Assembler language of an IMS DLI call that will send a string to the Guardium appliance:

```
MVC       IOAREA(20),=CL20'THIS IS AN APP_EVENT'    /Set APP_EVENT message
XC      PARM@(12*4),PARM@                           /Clear parameter area
LA       R1,GN                        /Addr of GN literal
ST             R1,PARM@+0                                    /Save in parmlist
L       R2,APPCB@                                            /Addr of AUIAPPEV PCB
ST      R2,PARM@+4                                  /Save in parmlist
LA      R1,IOAREA                                            /Addr of IOAREA
ST       R1,PARM@+8                  /Save in parmlist
OI      PARM@+8,X'80'           /Terminate parmlist
LA       R1,PARM@                 /Addr of parmlist
L       R15,DLI@                /Addr of ASMTDLI program
BASR    R14,R15                                               /Call ASMTDLI
```

C program

The following is an example of a C program:

```
#define    iopcb     (IO_PCB_TYPE *)(__pcblist)        /* I/O PCB */
#define    dbpcb     (PCB_STRUCT_8_TYPE *)(__pcblist)  /* DB PCB  */
#define    aepcb     (PCB_STRUCT_8_TYPE *)(__pcblist)  /* AUIAPPEV DB PCB  */

int  rc = 0;
const static char GU = "GU  ";

struct {
  char output 2000¨;
} iodata ;


....
....

/* create a APP_EVENT */
sprintf(iodata.output, "THIS IS AN APP_EVENT");
rc = ctdli(GU, aepcb, &iodata);
```

Parent topic: Configuring APP_EVENT support

Using agent configuration keywords to customize auditing

Some agent configuration keywords must be used for the product to function. You can also use agent configuration keywords for optional auditing specifications.

Required keywords

The following keywords must be set for the product to function:

APPLIANCE_SERVER
: This is the host name, or IP address, of the IBM Guardium system to which the agent should connect.

LOG_STREAM_DLIO
: This is the log stream name for online DLI calls.

LOG_STREAM_DLIB
: This is the log stream name for batch DLI calls.

You can also audit accesses to database-related data sets using SMF records. To audit accesses to IMS data sets that occur outside of IMS services, use the following keywords:

SMF_SPILL_FILE

This is the data set name.

SMF_DSN_MASK_1
This is the data set mask value.

Optional keywords

To set the following optional specifications, use the keyword that is listed. More information about each specification is provided, following this list.

Enabling Simulation mode
STAP_STREAM_EVENTS(N)

Restricting IMS segment and concatenated key data from being sent to the Guardium appliance
FORCE_LOG_LIMITED(Y)

Using multiple SMF data set masks
SMF_DSN_MASK_2 through SMF_DSN_MASK_10

Disabling SMF auditing at the agent level
SMF_CYCLE_INTERVAL(0)
Note: If SMF_CYCLE_INTERVAL(0) is specified, no additional SMF configuration parameters are required.

Controlling the frequency of SMF z/OS catalog queries
SMF_CYCLE_INTERVAL(time in minutes)

Changing the retention period of incomplete SMF events
SMF_EVENT_EXPIRY(number of days)

Changing the name of the SMF address space JCL
SMF_PROC_NAME(new name)

Auditing IMS data set access
SMF_SELF_AUDIT(Y)

Changing the type of events audited using SMF records
SMF_AUDIT_LEVELS(ALL|UPDATE|DELETE|READ|CREATE|ALTER|RACF)

Overriding the range of ports used for address space communications
LOG_PORT_SCAN_START(41501), LOG_PORT_SCAN_COUNT(24003)

Requesting specific agent messages to be issued to the operator console
WTO_MSG(AUIF507E), WTO_MSG(AUIT013I)

Determining the context of APPLIANCE_SERVER_[1-5] or APPLIANCE_SERVER_[FAILOVER|MULTI_STREAM|HOT_FAILOVER]_[1-5]
APPLIANCE_SERVER_LIST(FAILOVER|MULTI_STREAM|HOT_FAILOVER)

Providing Guardium system failover support
APPLIANCE_SERVER_FAILOVER_[1-5](IP address or host name)

Providing Guardium system multistream support
APPLIANCE_SERVER_MULTI_STREAM_[1-5](IP address or host name)

Providing Guardium system hot failover support
APPLIANCE_SERVER_HOT_FAILOVER_[1-5](IP address or host name)

Providing a spill area for short term outages
OUTAGE_SPILL_AREA_SIZE(megabytes)

Disabling IMS SLDS auditing at the agent level
IMSL_CYCLE_INTERVAL(0)
Note: If IMSL_CYCLE_INTERVAL(0) is specified, no additional IMSL configuration parameters are required.

Controlling the frequency IMS System Log Data Sets are allocated and read
IMSL_CYCLE_INTERVAL(time in minutes)

Changing the name of the IMSL address space JCL
IMSL_PROC_NAME(new name)

Changing the type of events audited using IMS SLDS records
IMSL_AUDIT_LEVELS(ALL|CTL_STRT|USERS|DBOPN|DB_PSB)

Changing the name of the Common Memory Management address space JCL
AUIU_PROC_NAME(new name)

Excluding DLI calls occurring on specific LPARS from being audited
AUIU_EXCLUDE_LPAR(lpar1, lpar2...lpar9)

Running more than one agent in a SYSPLEX
ADS_SHM_ID(100010), ADS_LISTENER_PORT(16055)

Removing Segment data and Concatenated Key values from audited data at the agent level
FORCE_LOG_LIMITED(Y)

Using the System z Integrated Information Processor (zIIP)
ZIIP_AGENT_DLI

Viewing AUI messages that are produced by the IMS Control regions in the AUI agent log
DISPLAY_IMSMSG_DLIO(N|Y)

Viewing AUI messages produced by the IMS DLI/DBB batch jobs in the AUI agent log
DISPLAY_IMSMSG_DLIB(N|Y)

Restricting auditing to specific IMS systems when multiple IMSs share RECON data sets
IMSNAME_EQ_IMSSSID(N|Y)

Enabling/Disabling the IBM Guardium S-TAP for IMS configuration value display at agent startup
TRACE_CONFIG(ON|OFF)

Setting the number of days within which AUILxxxx will process IMS system log data sets (SLDS)
IMSL_SLDS_SRCH(number of days)

- **Simulation mode**
  Simulation mode enables you to simulate agent processing. IBM Guardium S-TAP for IMS uses various z/OS MVS system services to gather audit data and move it to the agent address space. The agent address space evaluates this data according to the specified policy, and transmits the audit record to the Guardium appliance by using TCP/IP. To assess the impact on MVS processing, use the STAP_STREAM_EVENTS parameter to simulate data collection.
- **Specifying multiple SMF data set masks**
  You can use the SMF_DSN_MASK keyword to specify up to nine additional SMF data set masks.
- **Disabling SMF auditing at the agent level**
  You can use the SMF_CYCLE_INTERVAL keyword to disable SMF auditing at the agent level.

- **Controlling the frequency of SMF z/OS catalog queries**
  You can change the frequency of SMF z/OS catalog queries by using the SMF_CYCLE_INTERVAL keyword to specify a value in minutes:
- **Changing the retention period of incomplete SMF events**
  By default, incomplete SMF events will be retained in your SMF spill data set for 5 days. You can change this time range by specifying the SMF_EVENT_EXPIRY keyword:
- **Changing the name of the SMF address space JCL**
  To change the name of the AUIFS*TC* JCL member name, use the SMF_PROC_NAME keyword to change AUIFSTC to a name of your choice:
- **Auditing IMS data set access**
  To obtain a report of IMS artifact access, use the SMF_SELF_AUDIT keyword.
- **Changing the types of events that are audited using SMF records**
  Use the SMF_AUDIT_LEVELS keyword to indicate a list of events to be audited, instead of collecting all event types.
- **Using alternate RECON data sets for SMF and SLDS processing**
  You can optionally use copies of the IMS RECON data sets when processing SMF (AUIF*STC*) and IMS SLDS (AUIL*STC*) data instead of using the live RECON data sets.
- **Overriding the range of ports used for communication between address spaces**
  You can set the available port scan starting point and limit the number of ports to check for availability.
- **Overriding the TCP/IP DNS resolver table**
  IBM Guardium S-TAP for IMS uses TCP/IP as a host path for intra- and inter-address space communication of information such as collection policy details and address space status updates. To receive information from an AUIU*STC*_(Common Storage Management Utility) address space running on a different LPAR in the sysplex, the AUIA*STC*_(agent) address space must determine its own physical IP address and make it known to AUIU*STC*.
- **Specifying agent messages to issue to the operator console**
  You can use the WTO_MSG keyword to specify the messages to issue to the operator console.
- **Creating a spill area for short-term outages**
  Use the OUTAGE_SPILL_AREA_SIZE keyword and parameter to indicate the size in megabytes to allocate for the spill area.
- **Disabling IMS SLDS auditing at the agent level**
  You can turn off the auditing process that uses IMS SLDS records by specifying the IMSL_CYCLE_INTERVAL keyword with a value of zero.
- **Controlling the frequency with which IMS System Log Data Sets are allocated and read**
  You can specify the frequency of IMS RECON data set queries by specifying the IMSL_CYCLE_INTERVAL keyword.
- **Changing the name of the IMSL address space JCL**
  To change the JCL member name AUIL*STC*, use the IMSL_PROC_NAME keyword.
- **Changing the types of events audited using IMS SLDS records**
  To audit some, instead of all event types, you can specify each event type to be audited by using the IMSL_AUDIT_LEVELS keyword.
- **Changing the name of the Common Memory Management address space JCL**
  Use the AUIU_PROC_NAME keyword to change the member name from AUIU*STC* to a name of your choice.
- **Excluding DLI calls on specific LPARS from being audited**
  To stop the transmission of the AUIU*STC* address spaces to all LPARs, the AUIU_EXCLUDE_LPAR keyword can be used to exclude specific LPARS from the target list of eligible LPARS.
- **Running more than one agent in a SYSPLEX**
  If two or more IMS agents are running on one SYSPLEX, use the ADS_SHM_ID and ADS_LISTENER_PORT keywords to differentiate the shared memory segment and port for each agent environment.
- **Restricting auditing to specific IMS systems when multiple IMS systems share RECON data sets**
  If multiple unrelated IMS systems share RECON data sets, and you want to audit only on one or more specific IMS systems, use the keyword IMSNAME_EQ_IMSSSID(Y) to isolate auditing to the desired IMS system.
- **Using the System z Integrated Information Processor (zIIP)**
  You can use the System z® Integrated Information Processor (zIIP) when running IBM Guardium S-TAP for IMS Control region address space, and in the agent address space (AUIA*STC*). Use the ZIIP_AGENT_DLI keyword with the Y parameter to cause the agent to make a zIIP-enabled enclave SRB initialization attempt.
- **Using multiple Guardium systems**
  You can configure multiple Security Guardium systems for automatic failover. By configuring one or more backup systems, you ensure continuous auditing capability. This process is known as failover. You can also enable the streaming of audited data from one or more IBM Guardium S-TAP for IMS agents to up to 6 connected Security Guardium systems. This process is known as multistreaming.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Simulation mode

Simulation mode enables you to simulate agent processing. IBM® Guardium® S-TAP® for IMS uses various z/OS MVS system services to gather audit data and move it to the agent address space. The agent address space evaluates this data according to the specified policy, and transmits the audit record to the Guardium appliance by using TCP/IP. To assess the impact on MVS processing, use the STAP_STREAM_EVENTS parameter to simulate data collection.

When STAP_STREAM_EVENTS is set to *N*, the parameter stops the agent TCP/IP data transmission process. The agent performs all data collection processes but does not send the audit record to the Guardium appliance.

Parent topic: Using agent configuration keywords to customize auditing

Specifying multiple SMF data set masks

You can use the SMF_DSN_MASK keyword to specify up to nine additional SMF data set masks.

Specifying multiple SMF data set masks

The naming conventions of some environments prohibit the use of a SMF_DSN_MASK_1 value, which allows all required data sets to be read. To audit accesses to database-related data sets from multiple LPARS of your SYSPLEX, you can specify up to nine additional data set mask values: SMF_DSN_MASK_2 through SMF_DSN_MASK_10.

Parent topic: Using agent configuration keywords to customize auditing

Disabling SMF auditing at the agent level

You can use the SMF_CYCLE_INTERVAL keyword to disable SMF auditing at the agent level.

For any IMS systems that are audited by this agent, you can disable audit access to IMS data sets that occur outside the use of IMS services. To do so, specify the following keyword with the value of zero: SMF_CYCLE_INTERVAL(0)

Specifying SMF_CYCLE_INTERVAL(0) turns off auditing process that uses SMF records. The agent address space (AUIA*STC*) will not start the SMF auditing address space (AUIF*STC*).

Parent topic: Using agent configuration keywords to customize auditing

Controlling the frequency of SMF z/OS catalog queries

You can change the frequency of SMF z/OS catalog queries by using the SMF_CYCLE_INTERVAL keyword to specify a value in minutes:

To determine if any new, unread data sets match the specified SMF_DSN_MASK_x values, the SMF processing address space (AUIF*STC*) periodically performs a query against the z/OS catalog, looking for data sets to process. By default, this query is performed when the AUIF*STC* task is started, and repeated every 300 minutes (5 hours). To change the default time value, use the keyword SMF_CYCLE_INTERVAL*(time in minutes)*. If you specify a time value of zero, the SMF auditing feature will be disabled.
Parent topic: Using agent configuration keywords to customize auditing

Changing the retention period of incomplete SMF events

By default, incomplete SMF events will be retained in your SMF spill data set for 5 days. You can change this time range by specifying the SMF_EVENT_EXPIRY keyword:

In some situations, such as a canceled job or end-of-memory events, a type 30 record is not produced for a step or job. To keep these types of records from filling your SMF spill data set, you can set a time limit in days to determine how long incomplete SMF records are retained. The default value is 5 days and can be changed by specifying the SMF_EVENT_EXPIRY keyword to indicate the number of days of your choice: SMF_EVENT_EXPIRY*(number of days)*.
Parent topic: Using agent configuration keywords to customize auditing

Changing the name of the SMF address space JCL

To change the name of the AUIF*STC* JCL member name, use the SMF_PROC_NAME keyword to change AUIFSTC to a name of your choice:

AUIF*STC* is the name of the JCL that provides auditing of data set accesses using SMF records. AUIF*STC* is provided in the product installation sample data set (SAUISAMP). If the name AUIF*STC* conflicts with your site's naming convention standards, or if more than one agent is being used, you can change the name of this JCL. Use the SMF_PROC_NAME keyword to change the member name from AUIF*STC* to a name of your choice: SMF_PROC_NAME*(new name)*.

Ensure that this JCL resides in a procedure data set (PROCLIB) that allows the z/OS START command S taskname to be used.

Parent topic: Using agent configuration keywords to customize auditing

Auditing IMS data set access

To obtain a report of IMS artifact access, use the SMF_SELF_AUDIT keyword.

IBM Guardium S-TAP for IMS reads the IMS RECON data sets and system log data sets produced by IMS (SLDS) to obtain IMS environment information, such as IMS artifact names. IMS artifact names determine the databases and data sets that are used to create audit information.

By default, IBM Guardium S-TAP for IMS does not report accesses of IMS artifacts. To obtain a report of these accesses, specify a value of Y using the SMF_SELF_AUDIT keyword: SMF_SELF_AUDIT*(Y)*.

Parent topic: Using agent configuration keywords to customize auditing

Changing the types of events that are audited using SMF records

Use the SMF_AUDIT_LEVELS keyword to indicate a list of events to be audited, instead of collecting all event types.

When auditing using SMF records is enabled, the default action is to provide auditing for all of the following accesses to data sets:

- Open events with READ access
- Open events with UPDATE/WRITE access
- Open events with ALTER access
- Data set DELETE events
- Data set CREATE events
- Access denied (RACF violation)

To specify some and not all of these events for auditing, you can specify each type of event to be audited by using the SMF_AUDIT_LEVELS keyword: SMF_AUDIT_LEVELS (*ALL*|*READ*|*UPDATE*|*DELETE*|*CREATE*|*ALTER*|*RACF*).
Remember: This keyword affects the SMF auditing level for all IMS subsystems controlled by this agent. If you do not include READ accesses in the SMF_AUDIT_LEVELS parameter, then no READ accesses will be reported for any of the IMS environments that are audited by using the agent.
Note: You can separate parameters for the collection of different event types. For example, to audit UPDATE and READ events, include the UPDATE and READ records as follows:

```
SMF_AUDIT_LEVELS(UPDATE)
SMF_AUDIT_LEVELS(READ)
```

instead of:

```
SMF_AUDIT_LEVELS(UPDATE|READ)
```

Parent topic: Using agent configuration keywords to customize auditing

Using alternate RECON data sets for SMF and SLDS processing

You can optionally use copies of the IMS RECON data sets when processing SMF (AUIF*STC*) and IMS SLDS (AUIL*STC*) data instead of using the live RECON data sets.

To use alternate RECON data sets for SMF and SLDS processing:

1. Add a //AUIARCN DD statement to the AUIF*STC* and AUIL*STC* JCLs that contain the name of the IMS system (as defined in the IMS Definition panel of the Guardium interface).
2. Add the alternate RECON data set names to be used when processing these two types of data sources.
   Note: Specifying alternate RECON data set names only affects AUIF*STC* and AUIL*STC* task processing. It has no effect on processing of any other tasks.

Use IDCAMS, or another VSAM-compatible method, to create cataloged, VSAM copies of your live RECON data sets.

The data set that is specified by the AUIARCN DD statement must be defined as Fixed Block (FB) with a record length of 80 bytes (LRECL=80), and it can be a PDS, PDS/E, or sequential file. The following guidelines apply:

- An asterisk (*) in column 1 indicates that the line is a comment.
- Keywords must start in column 1.
- No spaces are allowed within keywords and parameters.
- Multiple IMSNAME keywords can be specified in one AUIARCN file.
- At least one RECON data set must be included under each IMSNAME identifier.
- Alternate RECON data sets must be cataloged and in IMS format.

Table 1. IMSNAME and RECON data set values, defined:

Value	Purpose
IMSNAME=	Specifies the IMS to which the subsequent RECON1, 2, and 3 keywords pertain.
RECON1=	Specifies the alternate data set name to be used for RECON1.
RECON2=	Specifies the alternate data set name to be used for RECON2.
RECON3=	Specifies the alternate data set name to be used for RECON3.

Example:

```
IMSNAME=IMSV14
RECON1=IMSEA1.ALT.RECON1
RECON2=IMSEA1.ALT.RECON2
RECON3=IMSEA1.ALT.RECON3
*
IMSNAME=IMSV13
RECON1=IMSDA1.ALT.RECON1
RECON2=IMSDA1.ALT.RECON2
```

Parent topic: Using agent configuration keywords to customize auditing

Overriding the range of ports used for communication between address spaces

You can set the available port scan starting point and limit the number of ports to check for availability.

IBM Guardium S-TAP for IMS uses a communications port to pass messages between threads within each address space. The default port is 41500. If the address space determines that port 41500 is not available for use, all subsequent ports up to 65535 are examined, and the first available port is used.
Some installations have restrictions on which ports should be examined and used. Use the LOG_PORT_SCAN _START and LOG_PORT_SCAN_COUNT keywords to set the available port scan starting point and limit the number of ports to be checked for availability:

- LOG_PORT_SCAN_START(41501)
- LOG_PORT_SCAN_COUNT(24003)

The sum of the value of the SCAN_START port number plus the SCAN_COUNT should not exceed 65535.
Parent topic: Using agent configuration keywords to customize auditing

Overriding the TCP/IP DNS resolver table

IBM Guardium S-TAP for IMS uses TCP/IP as a host path for intra- and inter-address space communication of information such as collection policy details and address space status updates. To receive information from an AUIU*STC*_(Common Storage Management Utility) address space running on a different LPAR in the sysplex, the AUIA*STC*_(agent) address space must determine its own physical IP address and make it known to AUIU*STC*.

To determine its physical IP address, the IBM Guardium S-TAP for IMS agent uses the z/OS getaddrinfo function and passes it to the LPAR name specified in the CVTSNAME field of the z/OS CVT control block. The getaddrinfo function uses the DNS resolver table to map the agent's LPAR name to its physical IP address. The DNS resolver table should contain entries that associate each LPAR within the sysplex to its physical IP address. If there is no association found, the agent (AUIA*STC*) uses the z/OS gethostname and getaddrinfo services to obtain the physical IP address of its own LPAR; but the IP addresses of other LPARs in the sysplex cannot be determined. In that case, inter-address space communication is not possible and events that occur on other LPARs are not reported to the Guardium appliance. Similarly, inter-address space communications can fail if users of Dynamic Virtual IP Addressing (VIPA) attempt to associate multiple IP addresses to a single VIPA token.

To determine if the LPAR name, in the CVTSNAME field, is included in the DNS table:

1. Run the Rexx executable that is located in the SAUISAMP data set of member AUIPING.
2. If the ping is successful, the LPAR name is defined in the DNS table and no further action is required.
3. If the ping fails due to an unknown host error, the LPAR name was not found in the DNS table. Contact your network administrator to request the addition of the LPAR name and the associated IP address to the DNS table.

Network administrators can manually associate the LPAR name that is found in the z/OS CVTSNAME field with the name that is used in the DNS revolver table by including the AUIHOST DD statement file in all IMS S-TAP agent task address space JCLs.

cvts_lpar_name(*dns_name*)

Required if AUIHOST DD is specified.
Default: None.
Description: Translates the CVTSNAME to the name in the DNS table.

lpar_name
Found in the z/OS CVTSNAME field.
Use the AUIPING REXX exec found in the SAUISAMP data set to obtain that name.
The *lpar_name* value can be from 1 -- 8 bytes in length.

dns_name
Found in the DNS table that associates the LPAR with an IP address.
The DNS_NAME value must conform to the following z/OS TCP/IP HOSTNAME rules:

- Must contain 1 or more tokens separated by a period.
- Each token must be at least 1 character and less than 64 characters.
- Each token must start with a letter or number.
- Remaining characters in each token must be a letter, number, or hyphen.

Example: PRODA(SYSTEM_1)
wherein:

- *PRODA* is the LPAR name found in the CVTSNAME field of your z/OS system
- *SYSTEM_1* is the mnemonic used in your DNS table to relate this LPAR to a TCP/IP address.

The AUIHOST DD statement file must meet the following standards:

- It must be a sequential file, or a member of a Partitioned Data Set (PDS) or Extended Partitioned Data Set (PDSE).
- It must be defined with a Fixed Blocked (FB) Record Format (RECFM).
- It must have a Logical Record Length (LRECL) of 80 bytes.
- Commented lines can be indicated by an asterisk (*) in column one or by a slash-asterisk (/*) in columns one and two.
- It must contain all host definitions on one line.
- Up to 16 DNS names can be specified.

The following is an example of an AUIHOST DD statement file:

```
MYLPAR20(MYLPAR20.mycompany.com)
MYLPAR21(MYLPAR21.mycompany.com)
MYLPAR22(MYLPAR22.mycompany.com)
MYLPAR23(MYLPAR23.mycompany.com)
MYLPAR24(MYLPAR24.mycompany.com)
MYLPAR25(MYLPAR25.mycompany.com)
MYLPAR26(MYLPAR26.mycompany.com)
```

Parent topic: Using agent configuration keywords to customize auditing

Specifying agent messages to issue to the operator console

You can use the WTO_MSG keyword to specify the messages to issue to the operator console.

IBM Guardium S-TAP for IMS allows you to specify informational, warning, or error messages to be written to the operator console. This allows an automated operations product to take some predefined action or provide a higher level of operator visibility to these messages. You can use the WTO_MSG to specify which messages should be write-to-operated.

- WTO_MSG(AUIF507E)
- WTO_MSG(AUIT013I)

You can specify one message ID per WTO_MSG instance. Messages originating from the AUIA*STC*, AUIF*STC*, AUIL*STC*, and AUIU*STC* address spaces are supported.
Parent topic: Using agent configuration keywords to customize auditing

Creating a spill area for short-term outages

Use the OUTAGE_SPILL_AREA_SIZE keyword and parameter to indicate the size in megabytes to allocate for the spill area.

Short-term communication outages between the agent address spaces and the IBM Guardium system can be handled by using a z/OS data space spill area. Use of the spill area can prevent the loss of audited data by allowing the z/OS agent to save audited data until the connection to the IBM Guardium system is restored. The restoration of the communications link results in the flushing of the data space contents to the IBM Guardium system.

Use the OUTAGE_SPILL_AREA_SIZE keyword and parameter to indicate the size in megabytes to allocate for the spill area: OUTAGE_SPILL_AREA_SIZE*(megabytes)*. If you specify zero or omit this keyword, the spill area will not be allocated or used. The maximum value you can specify is 1024 MB.

Parent topic: Using agent configuration keywords to customize auditing

Disabling IMS SLDS auditing at the agent level

You can turn off the auditing process that uses IMS SLDS records by specifying the IMSL_CYCLE_INTERVAL keyword with a value of zero.

For any IMS systems to be audited by this agent, you can disable audit events that are determined by reading IMS System Log Data Sets (SLDS). To disable the auditing process that uses IMS SLDS records, specify the following keyword with the value of zero: IMSL_CYCLE_INTERVAL*(0)*. The agent address space (AUIA*STC*) will not start the IMS SLDS auditing address space (AUIL*STC*).

Parent topic: Using agent configuration keywords to customize auditing

Controlling the frequency with which IMS System Log Data Sets are allocated and read

You can specify the frequency of IMS RECON data set queries by specifying the IMSL_CYCLE_INTERVAL keyword.

For the product to determine if any new, unread IMS System Log Data Sets LDS data sets have been created by the IMS Online system, the IMSL processing address space (AUIL*STC*) periodically performs a query against the IMS RECON data sets, looking for new SLDS. This query is performed when the AUIL*STC* task is started, and then by default, every 15 minutes. The frequency can be changed by providing a value in minutes by using the IMSL_CYCLE_INTERVAL keyword: IMSL_CYCLE_INTERVAL*(time in minutes)*

A value of zero will cause the IMS SLDS auditing feature to be disabled.

Parent topic: Using agent configuration keywords to customize auditing

Changing the name of the IMSL address space JCL

To change the JCL member name AUIL*STC*, use the IMSL_PROC_NAME keyword.

AUIL*STC* is the name of the JCL that is used to audit data sets using IMS SLDS records. AUIL*STC* is provided in the product installation sample data set (SAUISAMP). If this name conflicts with your site's naming convention standards, or if more than one agent is being used, you can change the name of this JCL.

Use the IMSL_PROC_NAME keyword to change the member name from AUIL*STC* to a name of your choice: IMSL_PROC_NAME*(new name)*

Ensure that this new JCL is in a procedure data set (PROCLIB) that allows the z/OS START command S taskname to be used.

Parent topic: Using agent configuration keywords to customize auditing

Changing the types of events audited using IMS SLDS records

To audit some, instead of all event types, you can specify each event type to be audited by using the IMSL_AUDIT_LEVELS keyword.

When you enable auditing by using IMS SLDS records, the default is to provide auditing for all of the following event types:

- IMS Online region starts and stops
- Users sign on/sign off
- Database Opens and Closes
- PSB|DBD start, stop, lock, unlock, and DBDDUMP

To audit only some of these events, you can specify each event type to be audited using the IMSL_AUDIT_LEVELS keyword: IMSL_AUDIT_LEVELS (*ALL*|*CTL_STRT*|*USERS*|*DBOPN*|*DB_PSB*).

This keyword governs the IMS SLDS auditing level for all IMS subsystems that are controlled by this agent. For example, if user signon/signoff is not included in the IMSL_AUDIT_LEVELS parameter, then no signon or signoff events will be reported from any of the IMS environments that are audited using the agent.

Note: You can separate parameters for the collection of different event types. For example, to audit CTL_STRT and DBOPN events, include the CTL_STRT and DBOPN records as follows:

```
IMSL_AUDIT_LEVELS(CTL_STRT)
IMSL_AUDIT_LEVELS(DBOPN)
```

instead of:

```
IMSL_AUDIT_LEVELS(CTL_STRT|DBOPN)
```

Parent topic: Using agent configuration keywords to customize auditing

Changing the name of the Common Memory Management address space JCL

Use the AUIU_PROC_NAME keyword to change the member name from AUIU*STC* to a name of your choice.

AUIU*STC* is the name of the JCL that is used to build filtering criteria in E/CSA on all LPARS of the SYSPLEX. AUIU*STC* is provided in the product installation sample data set (SAUISAMP). If this name conflicts with your site's naming convention standards, or if more than one agent is being used, you can change the name of this JCL.

Use the AUIU_PROC_NAME keyword to change the member name from AUIU*STC* to a name of your choice: AUIU_PROC_NAME*(new name)*.

Ensure that this JCL resides in a procedure data set (PROCLIB) that allows the z/OS START command S taskname to be used.

Parent topic: Using agent configuration keywords to customize auditing

Excluding DLI calls on specific LPARS from being audited

To stop the transmission of the AUIU*STC* address spaces to all LPARs, the AUIU_EXCLUDE_LPAR keyword can be used to exclude specific LPARS from the target list of eligible LPARS.

By default, the IBM Guardium S-TAP for IMS agent creates Common Memory Management address spaces (AUIU*STC*) on all LPAR members of a SYSPLEX. This allocates E/CSA memory, and inserts DLI call filtering criteria across all LPARS. A single agent monitors IMS control regions and DLI/DBB batch jobs running on any LPAR of the SYSPLEX.

If you do not want to transmit the AUIU*STC* address spaces to all LPARs, the AUIU_EXCLUDE_LPAR keyword can be used to exclude specific LPARS from the target list of eligible LPARS: AUIU_EXCLUDE_LPAR*(lpar1, lpar2...lpar9)*

The LPAR where the agent is running cannot be excluded. All other LPARS can be excluded by using the *ALL option in place of the LPAR name.

For example, AUIU_EXCLUDE_LPAR(*ALL).
Parent topic: Using agent configuration keywords to customize auditing

Running more than one agent in a SYSPLEX

If two or more IMS agents are running on one SYSPLEX, use the ADS_SHM_ID and ADS_LISTENER_PORT keywords to differentiate the shared memory segment and port for each agent environment.

The agent address space (AUIA*STC*) and subordinate address spaces (AUIF*STC* and AUIL*STC*) communicate by using a shared memory segment and communications port. Multiple agents require multiple unique shared memory segments and port values to ensure correct inter-address space communications. If you need to have two or more IBM Guardium S-TAP for IMS agents available on one SYSPLEX, the following keywords provide a method of uniquely identifying the shared memory segment and port for each agent environment:

- ADS_SHM_ID(100010)
- ADS_LISTENER_PORT(16055)

Specification of the ADS_SHM_ID and ADS_LISTENER_PORT requires the addition of a //AUICONFG DD statement to the AUIF*STC* and AUIL*STC* address space JCLs. This DD statement should point to the same data set and member as the AUIA*STC* and AUIU*STC* JCLs for the agent, to ensure that communications between all participant address spaces use the correct memory object and ports.

See Customizing the agent by using agent parameter keywords for complete descriptions of all valid parameters, including the ADS_SHM_ID and ADS_LISTENER_PORT keywords.

Parent topic: Using agent configuration keywords to customize auditing

Restricting auditing to specific IMS systems when multiple IMS systems share RECON data sets

If multiple unrelated IMS systems share RECON data sets, and you want to audit only on one or more specific IMS systems, use the keyword IMSNAME_EQ_IMSSSID(Y) to isolate auditing to the desired IMS system.

The default option, IMSNAME_EQ_IMSSSID(N), causes only the IMS RECON data sets to be used when IBM Guardium S-TAP for IMS attempts to find and match IMS systems to active audit policies.

Specifying IMSNAME_EQ_IMSSSID(Y) causes both the IMS RECON data sets, and the 8-byte IMS subsystem/DBCTL RSENAME to be used when IBM Guardium S-TAP for IMS attempts to find and match IMS systems to active audit policies.

Consider the following example:

RECON data sets A.B.C1/C2/C3 contain information for IMSA and IMSB. Auditing is only desired for IMSB. Policy AUDIT_ALL is installed by using IMS appliance definition *MY_IMS*, which references RECON data sets A.B.C1/C2/C3.

If subsystems IMSA and IMSB both use RECON data sets that are referenced by the policy, AUDIT_ALL, and associated with the IMS definition, *MY_IMS*, then both IMSA and IMSB are audited when the default, IMSNAME_EQ_IMSSSID(N), is specified.

To restrict auditing to IMSB:

1. Specify IMSNAME_EQ_IMSSSID(Y) in the AUICONFG file.
2. Name the IMS definition in the appliance `IMSB`.
3. Relate policy AUDIT_ALL to `IMSB`.
4. Install the policy.

As a result, IMSB is audited with the criteria that is set in policy AUDIT_ALL, and IMSA is not audited.
Note: DLI batch jobs (DLI/DBB) might not be tightly associated with an IMSID, therefore IBM Guardium S-TAP for IMS will report on all DLI batch jobs that use the audited RECON data set. The IMSNAME_EQ_IMSSID parameter does not affect DLI/DBB batch job auditing.
Parent topic: Using agent configuration keywords to customize auditing

Using the System z Integrated Information Processor (zIIP)

You can use the System z® Integrated Information Processor (zIIP) when running IBM Guardium S-TAP for IMS Control region address space, and in the agent address space (AUIA*STC*). Use the ZIIP_AGENT_DLI keyword with the Y parameter to cause the agent to make a zIIP-enabled enclave SRB initialization attempt.

IMS control region

The following processes are moved to the zIIP in the IMS Online Control Region, pending redirection by the operating system:

- DLI call filtering
- IXGWRITE of audited DLI call data to the z/OS System Logger log stream

To use a zIIP in the IMS Online Control region, add a //AUIZIIP DD DUMMY to the IMS control region JCL.

Agent address space

The following processes are moved to the zIIP in the agent address space (AUIA*STC*), pending redirection by the operating system:

- IXGBROWSE read of audited data from the z/OS System Logger log streams for both Online and Batch DLI calls
- TCP/IP send of the data to the Guardium system

To use a zIIP in the agent address space, use the ZIIP_AGENT_DLI keyword with the Y parameter to the configuration file that is pointed to by the AUICONFG DD statement in the agent JCL (AUIA*STC*).

Parent topic: Using agent configuration keywords to customize auditing

Using multiple Guardium systems

You can configure multiple Security Guardium systems for automatic failover. By configuring one or more backup systems, you ensure continuous auditing capability. This process is known as failover. You can also enable the streaming of audited data from one or more IBM Guardium S-TAP for IMS agents to up to 6 connected Security Guardium systems. This process is known as multistreaming.

- **Providing Guardium system failover**
  You can specify up to five additional Guardium systems to be connected to the agent by using the APPLIANCE_SERVER_FAILOVER_x keyword, where x = a digit between one and five.
- **Streaming to multiple Guardium systems**
  Multistream mode enables S-TAP audit events to be sent to multiple connected appliances. You can enable multistreaming to up to 6 IBM Guardium system (APPLIANCE_SERVER + APPLIANCE_SERVER_MULTI_STREAM_*n*, where *n* can be 1 - 5).
- **Keeping connections active when HOT_FAILOVER is enabled**
  When the HOT_FAILOVER feature is enabled by setting the APPLIANCE_SERVER_LIST parameter to *HOT_FAILOVER*, connections for each connected Guardium appliance are kept active by pings. (The following connection types are kept active: DLIO, DLIB, SMF, IMSL, and MLOG.)

Parent topic: Using agent configuration keywords to customize auditing

Providing Guardium system failover

You can specify up to five additional Guardium systems to be connected to the agent by using the APPLIANCE_SERVER_FAILOVER_x keyword, where x = a digit between one and five.

The failover process

IBM Guardium S-TAP for IMS uses the concept of a single primary IBM Guardium system and multiple secondary backup systems.

- When a primary IBM Guardium system goes offline, the IBM Guardium S-TAP for IMS agent automatically establishes a connection to a secondary IBM Guardium system, and the audited data is sent to the secondary system.
- When a primary IBM Guardium system comes back online, the IBM Guardium S-TAP for IMS agent detects it, and reestablishes the connection to the primary IBM Guardium system and restarts, sending data to the primary system.

This allows the use of any IBM Guardium system as a short-term backup, while always attempting to use the primary system as the main data storage medium.

In the following example failover scenario, where none of the systems are online, the IBM Guardium S-TAP for IMS agent attempts to connect to the primary IBM Guardium system at a regular interval and follows the usual failover logic if the primary IBM Guardium system is offline. A connection is reestablished to any of the configured appliances as soon as one becomes available.

Enabling multiple system failover support

IBM Guardium S-TAP for IMS allows the specification of up to five additional IBM Guardium system to be connected to the agent. This feature provides failover protection, which allows the agent to continue to send audited data to one of a number of backup IBM Guardium system in the event of a communication failure with the primary system. You must use the APPLIANCE_SERVER keyword to enable this feature, because the IBM Guardium system that is referenced by this keyword is the primary connection. You can specify additional IBM Guardium system by using the APPLIANCE_SERVER_FAILOVER_x keyword, where x = a digit from 1 to 5.

- APPLIANCE_SERVER_FAILOVER_1(IP address 1)
- APPLIANCE_SERVER_FAILOVER_2(host name 2)
- APPLIANCE_SERVER_FAILOVER_3(IP address 3)
- APPLIANCE_SERVER_FAILOVER_4(IP address 4)
- APPLIANCE_SERVER_FAILOVER_5(host name 5)

Example failover scenario

Audit data flows to the primary IBM Guardium system, A.

The TCP/IP connection from the IBM Guardium S-TAP for IMS agent to the primary IBM Guardium system fails.

A connection is made to the secondary IBM Guardium system, B.

Audit data is now flowing to the secondary IBM Guardium system, B.

The TCP/IP connection from the IBM Guardium S-TAP for IMS agent to the primary IBM Guardium system is reestablished.

Audit data now flows to the primary IBM Guardium system, A.

The IBM Guardium S-TAP for IMS agent and IBM Guardium system B disconnect.

Parent topic: Using multiple Guardium systems

Streaming to multiple Guardium systems

Multistream mode enables S-TAP audit events to be sent to multiple connected appliances. You can enable multistreaming to up to 6 IBM Guardium system (APPLIANCE_SERVER + APPLIANCE_SERVER_MULTI_STREAM_*n*, where *n* can be 1 - 5).

IBM Guardium S-TAP for IMS sends events to a single appliance until a ping occurs, or the number of records that is specified by MEGABUFFER_COUNT is reached. Audited DLI events are distributed amongst additional appliances in a round-robin sequence.

To enable multistreaming, you must specify *MULTI_STREAM* when you configure the APPLIANCE_SERVER_LIST parameter. The APPLIANCE_SERVER and APPLIANCE_SERVER_[MULTI_STREAM]_[1-5] parameters specify the appliances to which you intend to stream events. The appliance that is specified by APPLIANCE_SERVER provides the policy that is used for event matching.

Enabling multistream support

Use the APPLIANCE_SERVER keyword to enable multistream support. The IBM Guardium system that is referenced by the APPLIANCE_SERVER keyword is the primary connection, and it provides the policy used to match DLI events. You can specify additional appliances by using the APPLIANCE_SERVER_MULTI_STREAM_*n* keyword, where *n* is a digit from 1 - 5.

Specify up to 5 additional IBM Guardium system IP addresses or host names. For example:

- APPLIANCE_SERVER_MULTI_STREAM_1(IP address 1)
- APPLIANCE_SERVER_MULTI_STREAM_2(host name 2)
- APPLIANCE_SERVER_MULTI_STREAM_3(IP address 3)
- APPLIANCE_SERVER_MULTI_STREAM_4(IP address 4)
- APPLIANCE_SERVER_MULTI_STREAM_5(host name 5)

Parent topic: Using multiple Guardium systems

Keeping connections active when HOT_FAILOVER is enabled

When the HOT_FAILOVER feature is enabled by setting the APPLIANCE_SERVER_LIST parameter to *HOT_FAILOVER*, connections for each connected Guardium® appliance are kept active by pings. (The following connection types are kept active: DLIO, DLIB, SMF, IMSL, and MLOG.)

If the primary appliance becomes unavailable and failover occurs, the appliance policy that was originally pushed from the primary appliance continues to be active. When all Guardium appliances are connected, the status of each appliance connection, listed in the Guardium interface, is green.

Parent topic: Using multiple Guardium systems

IBM Security Guardium S-TAP for IMS on z/OS agent reference information

The IBM Guardium S-TAP for IMS agent provides access to database and appliance services, in support of the product's remote clients. The agent also reads audited DLI events placed in the z/OS System Logger log streams by the IMS Online and DLI/DBB batch Data collectors and sends the DLI events to the IBM Guardium system using TCP/IP connections.

- **Sample library members**
  Use the following sample library members shipped with IBM Guardium S-TAP for IMS to install and configure the product.
- **Agent environment**
  The agent must be running before you can use product functions related to the IMS subsystems monitored by that agent.
- **APF authorization**
  For security, the agent must be APF-authorized before it can be run.
- **Agent job output**
  The primary output of the agent job consists of log messages written to the AUILOG DD. These messages provide status information about the ongoing operation of the agent, and also record additional messages if errors occur.
- **Stopping the agent**
  When running on z/OS, the agent accepts standard z/OS /MODIFY and /STOP commands. When stopping the agent, all secondary address spaces controlled by the agent will also receive a stop request.
- **Starting and stopping the secondary address spaces**
  This topic describes the /MODIFY commands to start and stop the secondary address spaces.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Sample library members

Use the following sample library members shipped with IBM Guardium S-TAP for IMS to install and configure the product.

Table 1. Sample library members

Member	Type	Description
AUIAPPEV	DBD source statements	DBD source statements, used to define the optional APP_EVENT DBD
AUIA*STC*	JCL	Primary agent address space JCL
AUICONFG	CONFIG	Configuration file containing only the minimum required keywords
AUICONFX	CONFIG	Configuration file containing all available keywords
AUICPMOD	JCL	JCL to copy utility programs from SAUILOAD to SAUIIMOD data set
AUIEMAC1	MACRO	Edit macro to facilitate changes to other sample library members
AUIF*STC*	JCL	SMF data collection address space JCL

Member	Type	Description
AUIFUSPL	JCL	JCL to create the SMF incomplete event spill file for an agent
AUIL*STC*	JCL	IMS archived log data collection address space JCL
AUILSTR1	JCL	JCL to add CFRM structures for batch and online log streams to a CFRM policy
AUILSTR2	JCL	JCL to add batch and online log streams to your CFRM environment
AUILSTR3	JCL	JCL to add DASD-only log streams to your LOGR environment
AUIMIG10	JCL	JCL used to assist in the upgrade from V9.0 to V10.1.3
AUIMLOG	JCL	JCL used to read the IMS RECONS, detect missing logs, and send notification to the Guardium system
AUIPING	REXX EXEC	EXEC used to determine the LPAR name, as found in the CVTSNAME field, and issue a PING to determine if the LPAR name is in the network DNS table
AUISMFDF	JCL	JCL sample, showing the creation of a GDG file base for SMF data collection
AUISMFDP	JCL	JCL sample, showing the use of program IFASMFDP to filter SMF record types
AUITCPD	JCL	JCL used to generate a network diagnostic report
AUIU*STC*	JCL	Common storage management utility address space JCL

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS agent reference information

Agent environment

The agent must be running before you can use product functions related to the IMS subsystems monitored by that agent.

Important: Before the agent is started, system services should be started, and completely available for use. Examples of system services include JES, TCP/IP and the associated DNS RESOLVER, XCF, and the z/OS System Logger.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS agent reference information

APF authorization

For security, the agent must be APF-authorized before it can be run.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS agent reference information

Agent job output

The primary output of the agent job consists of log messages written to the AUILOG DD. These messages provide status information about the ongoing operation of the agent, and also record additional messages if errors occur.

In the event of exceptional conditions, additional messages might be written to the SYSOUT DD. If an abend occurs, dump information can be written to the CEEDUMP and SYSUDUMP DDs, if they are supplied. That information can be used in diagnosis by product support.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS agent reference information

Stopping the agent

When running on z/OS, the agent accepts standard z/OS /MODIFY and /STOP commands. When stopping the agent, all secondary address spaces controlled by the agent will also receive a stop request.

Important: System services, such as but not limited to the following, should remain available for use until the agent has completed termination: JES, TCP/IP and associated DNS RESOLVER, XCF and the z/OS System Logger.

From SDSF (or anywhere else that you can issue commands), you can issue one of these commands to the agent:

/STOP agent-job-name
: This is the recommended command to use to stop the agent. It initiates a graceful agent shutdown, which causes the agent to:

1. Wait for all existing requests to finish.
2. Exit.

/MODIFY agent-job-name,STOP
: Performs the same function as the /STOP agent-job-name command.

/MODIFY agent-job-name,FORCE
: This initiates an agent hard stop which causes the agent to:

1. Initiate hard cancels on all running threads.
2. Exit as soon as the threads exit.

Note: Use of the FORCE option can result in DUMP-producing ABENDS.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS agent reference information

Starting and stopping the secondary address spaces

This topic describes the /MODIFY commands to start and stop the secondary address spaces.

Commands to start and stop the SMF data collector address space

When the agent address space is started, secondary address spaces under the control of the agent may also be started. These include the SMF data collector address space (SAUISAMP member AUIF*STC*) which collects events using SMF log data as input and sends the events to the Guardium appliance. One IMS Archive Log event Data collector (SAUISAMP member AUIL*STC*) is also started for each IMS with an active collection.

Note: The following commands should be used against the agent's primary address space.

- /MODIFY <jobname>,START COLLECTOR SMF
- /MODIFY <jobname>,STOP COLLECTOR SMF

Optionally, the STOP command may be used to stop the SMF address space:

- /STOP <jobname>

Commands to start and stop the IMS Archive Log Data collector

There is no z/OS command to start the address space because the IMS Archive Log data collector address space is specific to an IMS definition with an active collection. The AUIL*STC* address is started by the agent address space, or activation of a collection.

Stopping a specific AUIL*STC* address space requires the use of the /STOP <jobname>.<token> command. The <token> value to be used can be found during AUIL*STC* startup in the AGENT JOBLOG.

In the following example, AAAAAAAC is the token value:

```
/S AUILRS22.AAAAAAAC
```

Or, when viewing the AUIL*STC* task in TSO SDFS, the token is displayed as the STEPNAME.
Parent topic: IBM Security Guardium S-TAP for IMS on z/OS agent reference information

Data collection

The collection process involves the gathering of audit event data at run time. Specify various filtering criteria to capture all relevant events and limit the amount of data that is collected and stored.

IBM Guardium S-TAP for IMS gathers audited events from the following sources:

- IMS database DLI calls performed from within IMS Online Control regions and DLI/DBB batch jobs
- SMF records
- IMS Log records from IMS System Log Data Sets (SLDS).

A single policy containing selection criteria that indicates the events to be audited, is applied to each source.

- **IMS database DLI calls**
  IBM Guardium S-TAP for IMS can filter audit events generated by database DLI calls by the following call types: Read, Update, Insert, and Delete.
- **SMF records**
  IBM Guardium S-TAP for IMS allows the filtering of audit events generated by access methods outside of IMS DLI services, including z/OS access methods such as VSAM or QSAM requests generated from z/OS batch jobs or TSO.
- **Records from IMS system log data sets (SLDS)**
  IBM Guardium S-TAP for IMS allows the filtering of audit events that are generated by IMS Online Control regions, which are logged to IMS log data sets and are processed from within the AUIL*STC* started task.
- **Filtering stages**
  Stage 0, Stage 1, and Stage 2 filtering is available for Collector Agent audit event collection when processing DLI calls.
- **Policy pushdown**
  This topic describes the policy pushdown process of mapping policies to an IBM Guardium S-TAP for IMS collection profile.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

IMS database DLI calls

IBM Guardium S-TAP for IMS can filter audit events generated by database DLI calls by the following call types: Read, Update, Insert, and Delete.

Note: Database DLI calls that do not result in a DBPCB status code of blanks, GA, or GK, are not audited unless the IMS policy indicates that one or more non-blank DLI codes should be reported. DLI calls performed using an IOPCB or TPPCB are not audited.

Database DLI calls issued from specific PSBs and user IDs can be included or excluded from auditing. PSB names and user IDs can be specified for auditing using fully qualified names, or by using wildcard characters.

Further filtering can be performed by including or excluding specific database and segment names. Wildcard support is available for both the database and segment name.

When auditing IMS DLI calls, you can obtain the concatenated key value of segments that are audited for all or specific database DLI calls, as well as the segment data for UPDATE, and INSERT calls. The segment data can also be obtained for READ and UPDATE calls where these calls are logically linked in the Guardium appliance to provide a before and after image of updated segments.

Parent topic: Data collection

SMF records

IBM Guardium S-TAP for IMS allows the filtering of audit events generated by access methods outside of IMS DLI services, including z/OS access methods such as VSAM or QSAM requests generated from z/OS batch jobs or TSO.

Some IMS Database Batch Utilities access IMS databases using access methods other the IMS Database DLI calls. As a result, the source of auditing records for these batch jobs will be the SMF records produced.

These audit events are based on z/OS SMF records and are processed from within the AUIF*STC* agent subtask. Policy criteria input for SMF data auditing is the same as for IMS DLI calls, but because of the nature of the SMF data, it is used differently.

The following data is not relevant, and therefore not used:

- DLI calls types
- PSB names
- Segment names

Database names are relevant because SMF data is based on data set names (part of the process that converts a policy to a filter, examines the IMS RECON data sets for artifacts in the RECON which relate to the INCLUDED database). These artifacts include database data set names (DSG/AREA/ADS) and database image copy data sets for each database data set. The AUIF*STC* tasks also audit other IMS related data sets.

By default, these data sets have been included because changes to these data sets can have an effect on data integrity:

- IMS RECON data sets
- Logging data sets generated by IMS DLI/DBB batch jobs
- SLDS/RLDS data sets
- IMS Online log data sets (OLDS)

It is possible to ignore the auditing of these data set types, as well as the database image copy data sets, by adding a DUMMY DD statement to the AUIF*STC* JCL. This table lists the data sets and corresponding DD DUMMY statement to include in the AUIFSTC JCL if you want to exclude the auditing of each of these types.

Table 1. Data sets and DD DUMMY statements

Data set Type	IMS RECONS	IMS LOGS	IMS OLDS	DB Image Copies
DD NAME	AUINRCN	AUINLOG	AUINOLD	AUINICS

Specify filtering of SMF events at the agent level, using access type or security violation, with the use of the SMF_AUDIT_LEVELS keyword in the configuration file. The keyword is pointed to by the AUICONFG DD statement of the agent (AUIA*STC*) JCL. Data set accesses to be audited are:

- OPEN for Read/Update
- Data set Alter/Create/Delete
- Any security product (such as RACF®) violations

The auditing of these accesses can be specified at the agent level (for example, all IMS systems defined to the agent), or at the IMS level. See the *Changing the type of events audited using SMF records* section for more details.

Parent topic: Data collection

Records from IMS system log data sets (SLDS)

IBM Guardium S-TAP for IMS allows the filtering of audit events that are generated by IMS Online Control regions, which are logged to IMS log data sets and are processed from within the AUIL*STC* started task.

Policy criteria input for IMS Log data auditing is the same as for IMS DLI calls, but is used differently because of the nature of IMS log data:

- DLI calls types are not relevant and therefore not used.
- Segment names are not relevant and therefore not used.
- PSB names are checked only when relevant to the event being examined.
- User IDs are checked only when relevant to the event being examined.
- DBD names are checked only when relevant to the event being examined.

In addition to filtering performed using the policy criteria, you can further filter IMS log data by event types, using the Guardium user interface. Using the IMSL_AUDIT_LEVELS keyword, you can set specific events to be audited, including:

- IMS Control Region Starts and Stops
- USER signon and signoffs
- Database OPEN/CLOSE
- DBD and PSB STARTS/STOPS/LOCK/UNLOCK

Occurrences of the DB DBDUMP command can also be audited. Auditing of these events can be specified at the agent level (for example, all IMS systems defined to the agent), or at the IMS level (for example, only for a specific IMS system). For more information, see *Changing the types of events audited using IMS SLDS records*.

Parent topic: Data collection

Filtering stages

Stage 0, Stage 1, and Stage 2 filtering is available for Collector Agent audit event collection when processing DLI calls.

Filtering occurs at one or more of the stages, 0, 1, and 2, depending on what fields are included in your filter. As many audit events as possible are filtered at the earliest possible stage (0, 1, or 2). You can control filtering performance by the fields you include in the rules for the active collection profile.

- **Stage 0 filtering**
  Stage 0 filtering occurs immediately after IMS executes the DLI call and it is determined that the call is a candidate for auditing, meaning one of the supported DLI call types and blanks, or another acceptable DLI status code, is returned.
- **Stage 1 filtering**
  Stage 1 filtering occurs through the use of USERID and PSB name values.
- **Stage 2 filtering**
  Stage 2 filtering occurs through the use of a filtering program that is compiled at the time of policy installation, using the criteria specified in the policy.

Parent topic: Data collection

Stage 0 filtering

Stage 0 filtering occurs immediately after IMS executes the DLI call and it is determined that the call is a candidate for auditing, meaning one of the supported DLI call types and blanks, or another acceptable DLI status code, is returned.

IBM Guardium S-TAP for IMS checks for an active policy for the IMS subsystem and determines if any rules governed by the active policy require the auditing of the DLI call type. If no policy is active, or no rules require the auditing of the DLI call type, processing control is returned to the application program. This is the most efficient form of filtering and should be used when possible.

Consider this example, wherein an active policy contains three rules:

- One rule only addresses INSERT requests.
- The second rule only addresses DELETE requests.
- The third rule only addresses UPDATE requests.

In this example, the READ DLI call is performed, and returns a status code of blanks. Since IBM Guardium S-TAP for IMS determines that no rules in the policy can reference a READ, processing control returns to the application program.

If the event that the DLI call performed in the example was an INSERT request, Stage 1 filtering would be invoked.

Parent topic: Filtering stages

Stage 1 filtering

Stage 1 filtering occurs through the use of USERID and PSB name values.

For Stage 1 filtering to occur, all rules of the active policy must contain identical USERID and PSB name values. Any inconsistencies in these values between rules prevents Stage 1 filtering from occurring.

Stage 1 filtering allows DLI calls that should be rejected, due to USERID or PSB name, to be excluded from the list of values to be audited. This can be due to the items not being included, or being intentionally excluded.

The determination that the USERID or PSB is causing the DLI call to be rejected is made by call to the Stage 2 compiled filters. The call to the Stage 2 complied filters is made when the USERID or PSB name of the current DLI call is not the same as the USERID or PSB name of the previous DLI call made in the same processing region.

In this example, the processing flow is demonstrated when discussing a BMP:

- The first DLI call is made and passes through Stage 0 processing.
- Stage 2 filtering is invoked, and it is determined that DLI calls from this USERID should not be audited. The DLI call is not audited, and control is returned to the application program.
- The next DLI call is made, and the USERID is the same as the previous DLI call in the region. The previous DLI call was not audited due to the USERID value, therefore this DLI call will not be audited.
- This process continues until the BMP STEP terminates with only one DLI call going through to Stage 2 filtering, and the remaining DLI calls are rejected during Stage 1 processing.

The same benefit can be seen with DLI and DBB batch jobs, because the USERID and PSB will not change during the execution step.

This process benefits online transactions and other processing threads where multiple DLI calls are performed from within a single unit-of-work, as well as when DLI calls are performed using C and D IMS command codes where multiple segments are affected by a single DLI call and auditing might be required on more than one segment within the hierarchical path.

Parent topic: Filtering stages

Stage 2 filtering

Stage 2 filtering occurs through the use of a filtering program that is compiled at the time of policy installation, using the criteria specified in the policy.

All DLI calls that are not rejected by Stage 0 and Stage 1 filtering are processed by the compiled filter. The compiled filter determines if the DLI call is to be audited based on all the policy criteria including DBD and segment name.

If the DLI call is to be audited, additional information is returned by the compiled filter, such as if the segment data and concatenated key should be included in the audited data block.

Parent topic: Filtering stages

Policy pushdown

This topic describes the policy pushdown process of mapping policies to an IBM Guardium S-TAP for IMS collection profile.

When the IBM Guardium S-TAP for IMS agent starts, it establishes a dedicated connection to the Guardium appliance for the reading of installed policies. Immediately after the connection is established, any installed policies are pushed down to the IBM Guardium S-TAP for IMS agent by the Guardium appliance. The Guardium appliance pushes down a full policy to all connected IBM Guardium S-TAP for IMS agents each time a policy is installed or uninstalled from the Guardium appliance.

Upon receipt of a policy, the IBM Guardium S-TAP for IMS agent compares the applicable rules with the existing collections, and performs a differential install.

Differential install
: A differential install of the policy indicates that only policies that have been modified since the last install are acted upon.

The following processing occurs in the IBM Guardium S-TAP for IMS agent upon receipt of a policy:

- The new policy is compared to the currently active policy if the new policy contains one or more rules.

    - If the policies are identical, no further processing is required.
- If the new policy does not apply to this subsystem, processing continues without any changes.
    - If there is an active policy, the collection continues using it.
    - If no policy is active, none is started.

Parent topic: Data collection

Creating and modifying IMS definitions

An IMS definition establishes a connection from your Guardium system to the IMS environment that you want to audit. To create and modify IMS definitions from the Guardium system interface, the agent address space (AUIA*STC*) must have a preestablished connection to the Guardium system.

- **Navigating to the IMS Definitions panel**
  IMS definitions can be created, modified, and deleted from the IMS Definitions panel of the Guardium system interface.
- **IMS Definition fields**
  The following fields are available in the IMS Definitions panel for your use in definition an IMS entry. Required fields are indicated with an asterisk.
- **IMSPLEX data sharing and XRF considerations**
  When you are considering IMS data sharing and XRF systems, take the following IMSPLEX data sharing and XRF considerations into account.
- **Adding an IMS definition**
  Add an IMS definition to the IMS Definitions List to include a defined IMS environment in the list of environments to be audited.
- **Modifying an IMS definition**
  You can modify the attributes that are set for an IMS definition on the IMS Definitions List.
- **Deleting an IMS definition**
  Delete an IMS definition from the IMS Definitions List to remove the IMS entry from the list of IMS environments to be audited.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Navigating to the IMS Definitions panel

IMS definitions can be created, modified, and deleted from the IMS Definitions panel of the Guardium system interface.

Procedure

1. From the Administration Console tab, select the Local Taps menu.
2. Select the IMS Definitions option.

Parent topic: Creating and modifying IMS definitions

IMS Definition fields

The following fields are available in the IMS Definitions panel for your use in definition an IMS entry. Required fields are indicated with an asterisk.

IMS Name

*IMS Entry Name
: A unique 1 - 8 character name to identify this IMS entry.

Description
: An optional description of the IMS Entry.

*Agent Name
: The name of the agent that audits this IMS entry.

RECONs

The RECON data set names are used to logically link the IMS definition, the active policy, the IMS Online Control region, and the DLI/DBB batch jobs that are running on z/OS, to audit the correct IMS instances.

*RECON1 Data Set Name
: The RECON1 data set name that is used by IMS on z/OS.

*RECON2 Data Set Name
: The RECON2 data set name that is used by IMS on z/OS.

RECON3 Data Set Name
: The RECON3 data set name that is used by IMS on z/OS.

IMS Data Sets

The IMS RESLIB data sets are used to determine the IMS release, during processing of the IMS System Log Data Sets (SLDS), using the AUIL*STC* address space. If more than one data set name is required, the data set names can be delimited by a comma.

*RESLIB Data Set Names
: A data set containing the IMS DFSVC000 module.

AUII050I Message Frequency
: Message AUII050I provides the number of DLI calls that are considered for auditing, and the number of DLI calls that were audited, based on the auditing criteria of the active policy. This message is produced based on the number of DLI calls that are considered, based on the following formula:

  Number of DLI calls in thousands (K) or Millions (M)

  or, by using both the formula and the time interval since the last AUII050I message was issued.

Example: If you provide values of `100K` (Number of DLI calls = 100,000) and `0100` (time interval of 1 hour), message AUII050I is issued when 100,000 DLI calls are seen by the product code, or by the 1 hour time interval, whichever comes first. The DLI counts and time interval reset when message AUII050I is issued.

Number of DLI calls
    xxx K|M
Time Interval
    HH:MM

Auditing Levels

Auditing levels can be set for both IMS Log and SMF events. For an explanation of the levels of auditing that are available for IMS Log and SMF events, see Configuration overview for a description of the IMSL_AUDIT_LEVELS and SMF_AUDIT_LEVELS configuration keywords.

IMS LOG Events
    Audit All IMS Log Events
    Audit Control Region Starts/Stops
    Audit User Signon/Signoff
    Audit DBD Open/Close
    Audit DBD/PSB/DUMP/START/STOP/LOCK/UNLOCK
SMF Events
    Audit All SMF Events
    Audit Dataset Open for Update
    Audit Dataset Deletes
    Audit Dataset Open for Read
    Audit Dataset Create
    Audit Dataset Alter
    Audit Dataset RACF® Violations

Parent topic: Creating and modifying IMS definitions

IMSPLEX data sharing and XRF considerations

When you are considering IMS data sharing and XRF systems, take the following IMSPLEX data sharing and XRF considerations into account.

IMSPLEX Data Sharing Considerations

Regardless of the number of LPARS that are involved, only one IMS definition is required in an IMS data sharing environment where all databases are shared by multiple IMS subsystems.

In an IMS data sharing environment where only a subset of databases is shared, an IMS definition must be created for each IMS subsystem with nonshared databases to be audited.

XRF Considerations

Only one IMS definition is required in an IMS XRF environment. IBM Security Guardium S-TAP for IMS on z/OS is not sensitive to which XRF partner is currently active. The product continues to produce audit data in the event of an XRF ACTIVE/BACKUP switch.

Parent topic: Creating and modifying IMS definitions

Adding an IMS definition

Add an IMS definition to the IMS Definitions List to include a defined IMS environment in the list of environments to be audited.

Procedure

1. From the IMS Definitions List, select the Add symbol, indicated by a plus sign, to the list of defined IMS systems.
   Enter the information in the IMS Definitions panel to define the new IMS environment to be audited.
2. Select Apply to save the new IMS definition.

Parent topic: Creating and modifying IMS definitions

Modifying an IMS definition

You can modify the attributes that are set for an IMS definition on the IMS Definitions List.

Procedure

1. Select the entry that you want to modify.
2. Modify the IMS definition fields.
3. Select Apply to save your changes.

Parent topic: Creating and modifying IMS definitions

Deleting an IMS definition

Delete an IMS definition from the IMS Definitions List to remove the IMS entry from the list of IMS environments to be audited.

About this task

IMS definitions can be deleted if no active IMS policies reference the IMS definition name. Only IMS definitions that are not part of an installed policy can be deleted.

Procedure

1. From the IMS Definitions List, select the IMS Definition that you want to delete.
2. Click the Delete icon.
   Click OK in the confirmation message to confirm the IMS entry deletion.

Parent topic: Creating and modifying IMS definitions

Reference information

This chapter provides IBM Guardium S-TAP for IMS reference information.

- **Data collection monitors**
  IBM Guardium S-TAP for IMS collects data from IMS online and batch activities, SMF, IMS archived logs, and IMS RECON data sets, by using the following internal product monitors.
- **IMS Log types and SMF record types that are collected by IBM Guardium S-TAP for IMS**
  The following tables show the IMS log types and SMF records types and descriptions that are collected by IBM Guardium S-TAP for IMS.
- **Fields that are used for IMS policy pushdown**
  The following fields defined in the Guardium system Access Rule Definition panel are used by IBM Guardium S-TAP for IMS to create policies and rules. Use the following information as a guideline.
- **Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS**
- **Echoed XML statement definitions**
  IBM Guardium S-TAP for IMS echoes the XML statements that are produced by the Guardium appliance to represent an Audit Policy. These statements are issued to a physical data set, agent AUILOG DD, or both, as determined by the XML_ECHO_DATASET and XML_ECHO_AUILOG parameters. This topic provides definitions of all XML statements that could be echoed from the appliance by the S-TAP.

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Data collection monitors

IBM Guardium S-TAP for IMS collects data from IMS online and batch activities, SMF, IMS archived logs, and IMS RECON data sets, by using the following internal product monitors.

IMS Online Activity Monitor
: The IMS Online Activity Monitor interfaces with IMS DL/I Language call analyzer module (DFSDLA00), and the IMS/VS Fast-Path Inter-region Communications Controller module (DBFIRC10), in order to be sensitive to the DL/I call type, and to access the data that is necessary for producing an audited event. When an INIT call is made to the IMS logger Exit routine (DFSFLGX0), interfaces to the IMS modules are activated, and they remain active until the DFSFLGX0 routine receives a TERM notification.
  For the activity monitor to be recognized by the IMS Online region, the IMS control region must be stopped and restarted with the SAUIIMOD data sets included as the first data sets in the STEPLIB DD concatenation.
  The IMS Online Activity Monitor and the agent communicate data collection criteria by using E/CSA control blocks. Determination of which DL/I calls and databases/segments is made at the time the DL/I call is performed, by using information that is derived from the data collection policy that is created through the IBM Guardium system's Access Rule definition process.
  The z/OS System Logger transports the audit data from the IMS Online Activity Monitor to the agent. All IMS online systems that are controlled by an agent use the same z/OS System Logger log stream. This z/OS system log stream is unique to the agent, and only contains audited events from IMS Online regions.

IMS Batch Activity Monitor
: The IMS Batch Activity Monitor interfaces with IMS DL/I language call analyzer module (DFSDLA00) in order to identify the DL/I call type and data that is necessary to produce an audited event. When the IMS Batch Exit routine (DFSISVI0) is invoked, the interface with the DL/I call analyzer is activated, and remains active until the batch step terminates.
  The IMS Batch Activity Monitor and the agent use E/CSA control blocks to communicate data collection criteria. The DLI calls and databases/segments determination is made at the time the DL/I call is performed, by using information that is derived from the data collection policy, which is created on the IBM Guardium system. The audit data from the IMS Batch Data Collector to the agent is transported through the z/OS System Logger.
  All IMS batch jobs that are controlled by an agent use the same z/OS System Logger log stream. This z/OS system log stream is unique to the agent, and only contains audited events from IMS Batch jobs.

IMS Online and Batch Data Collectors
: The IMS Online and Batch Data Collectors run as separate threads under the control of the agent address space (AUIA*STC*). The function of the data collector is to read audited events from the z/OS System Logger log stream, and send the events to the IBM Guardium system for storage by using a TCP/IP connection.
  Each thread maintains its own persistent TCP/IP connection to the Guardium system.

SMF Data Collector
: The SMF Data Collector reads a subset of SMF records from SMF memory dump data sets to determine whether data sets associated with audited IMS artifacts were read, written, deleted, or renamed. Security violations against these data sets can also be reported.
  IMS artifact associated data set types include database data sets, database image copy data sets, IMS log data sets (OLDS, SLDS and RLDS), and RECON data sets. The list of IMS artifact data sets to be monitored during SMF data collection is derived from the data collection policy that is created through the IBM Guardium system.
  As the processing of the SMF data sets is deferred, the data collection policy in force at the time of the SMF data set READ is the collection policy used, not the data collection policy in effect when the SMF event occurred. The names of the SMF memory dump data sets to be read is based on one or more SMF data set MASK values that are supplied by the use of one or more SMF_DSN_MASK keywords in the agent configuration file (AUICONFG). The data set names to that the SMF MASK refers reflects the SMF memory dump data sets that are created during offloading of the SMF recording data sets, or a copy of these data sets containing a subset of SMF record types that are created explicitly for the use of this product.
  Because an agent can monitor SMF events from all LPARS within a SYSPLEX, all SMF data sets to be read must be accessible from the LPAR on which the agent runs. The SMF Data Collector periodically queries the z/OS catalog for new data set names that meet the SMF MASK value. When cataloged data sets are found, these data sets are dynamically allocated and read by the SMF Data Collector. Auditable events that are found are formatted, and sent to the IBM Guardium system by using a TCP/IP connection.

The SMF Data Collector creates and maintains its own TCP/IP connection to the IBM Guardium system. The frequency that the SMF Data Collector queries the z/OS catalog is determined by the option you set during configuration of this product. The SMF Data Collector can be configured to audit only a subset of events by use of available options when configuring the agent and defining the IMS appliance through the Guardium system interface. The SMF Data Collector is run as a started task under the control of the agent. An example of the JCL for this started task can be found in the SAUISAMP data set in the AUIF*STC* member.
Note: IBM Guardium S-TAP for IMS only reports audited events for SMF record types that are collected by SMF. If specific SMF record types are not collected by your appliance or SMF recording data set memory dump utility, the event cannot be reported. Refer to the IMS Log types and SMF record types that are collected by IBM Guardium S-TAP for IMS topic for a list of SMF record types that are used by IBM Guardium S-TAP for IMS.

IMS Archived Log Data Collector

The IMS Archived Log Data Collector reads IMS Archived Log data sets (SLDS) and provides audit information about the following actions:

- IMS user signon and signoff
- IMS online region starts and stops
- Changes to the status of DBDs and PSBS within the IMS Online environment

The list of IMS artifacts to be monitored during IMS Archived Log collection is derived from the data collection policy you create, by using the Guardium system. As the processing of the IMS Archived Log sets is deferred, the data collection policy in force at the time that the IMS Archived Log data sets are read is the collection policy used (as opposed to the data collection policy in effect when the IMS Archived Log event as written to the IMS log data set).
The IMS Archived Log Collector periodically queries the DBRC RECON data sets that are associated with an IMS that is defined to IBM Guardium S-TAP for IMS to determine if new SLDS data sets were created since the last RECON data set query. New data sets that are found are dynamically allocated and read. Audited events are sent to the IBM Guardium system by using a TCP/IP connection.
The IMS Archive Log Data Collector can be configured to audit only a subset of events, by using the options available when configuring the agent and defining the IMS appliance through the Guardium system interface. The IMS Archived Log Data Collector is run as a started task under the control of the agent. An example of the JCL for this started task can be found in the SAUISAMP data set in the AUIL*STC* member.
IBM Guardium S-TAP for IMS starts one AUIL*STC* task for each set of RECON data sets that is actively monitored with a data collection policy.

- If an IMS data sharing environment with five IMS subsystems that share a single set of RECON data sets exists, only one AUIL*STC* task is started.
- If two separate IMS subsystems by using two separate sets of RECON data sets are being monitored, two separate AUIL*STC* tasks are started.
  Note: To collect events from the IMS archived logs, the DFSSLOGP (Primary Output SLDS) data set must be created and cataloged by your IMS Log Archive Utility process (program DFSUARC0).

IBM Guardium S-TAP for IMS dynamically starts and stops the appropriate number of AUIL*STC* tasks as required.

IMS Missing Log Utility

The IMS Missing Log Utility analyzes IMS RECON data sets to confirm the existence of SLDS/RLDS data sets. This function can be included or excluded, as well as scheduled without regard to the execution cycle setting for the AUIL*STC* task. This utility is run by a job or started task (see SAUISAMP member AUIMLOG for an example). It processes the RECON data sets of IMS systems with active policies audited by the agent and pointed to by the configuration member that is defined in the AUICONFG DD statement in the AUIMLOG JCL. The IMS RECON data sets are analyzed in search of IMS SLDS and RLDS data sets. If these are found, the z/OS appliance catalog is queried by using the SLDS/RLDS data set name. If the SLDS/RLDS data set is not found, a missing log event is sent to the IBM Guardium system.
Note: The AUIMLOG utility must be run under the same user ID, and on the same LPAR, as the AUIA*STC* task.

Common Storage Management Utility

IBM Guardium S-TAP for IMS uses memory in E/CSA to provide information regarding active data collection policies to the IMS Batch and Online Activity Monitors. An IBM Guardium S-TAP for IMS agent can be called to monitor IMS Online regions or DL/I batch jobs on many LPARS within a SYSPLEX. A started task is generated for execution on all LPARS of a SYSPLEX to read all active data collection policies and build the appropriate E/CSA control blocks. This started task is run when the IBM Guardium S-TAP for IMS agent starts and stops, as well as when a change is made to the state of any collection policy. An example of the JCL for this started task can be found in the SAUISAMP data set in the AUIUSTC member.
The LPARs where the AUIU*STC* task is run might be limited by adding the AUIU_EXCLUDE_LPAR keyword and LPAR names to the configuration file, which is specified by the AUICONFG DD statement in the AUIA*STC* JCL.

Parent topic: Reference information

IMS Log types and SMF record types that are collected by IBM Guardium S-TAP for IMS

The following tables show the IMS log types and SMF records types and descriptions that are collected by IBM Guardium S-TAP for IMS.

Table 1. IMS Logtypes collected by IBM Guardium S-TAP for IMS

Log type number	IMS log type	IMS log type description
06	IMS/VS Accounting Record X'06'	IMS Online was started or stopped.
16	A /SIGN command was successfully completed.	A /SIGN command successfully completed.
20	A database was opened.	A database was opened.
21	A database was closed.	A database was closed.
4C	DB/PSB Activity	Activity that is related to database or PSB processing
59xx	DEDB ADS OPEN Log record	DEDB area data set was opened.
5922	DEDB ADS CLOSE Log record	DEDB area data set was closed.
5923	DEDB ADS STATUS Log record	DEDB area data set status was changed.

SMF is used to obtain additional data set activity that is related to the monitored IMS databases and image copies.

Table 2. SMF record types and descriptions

SMF record Number	Type
00	IPL record
14	INPUT or RDBACK data set activity
15	OUTPUT, UPDATE, INOUT, or OUTIN data set activity
17	Scratch data set status
18	Rename non-VSAM data set
30	Common address space work, accounting information
60	VSAM volume data set updated
61	ICF catalog entry define

SMF record Number	Type
62	VSAM component or cluster opened
65	ICF delete activity
66	ICF alter activity
80	RACF® operator record
89	Usage data

Note: When image copies are read, they are collected as SMF type 14. When image copies are written, they are collected as SMF type 15. Image copies are sequential files, with some exceptions. If the image copy is opened as a VSAM file, the image copy is collected as SMF type 60.
Remember: IBM Guardium S-TAP for IMS can only report events that are being collected by SMF. If an SMF record type in this table is not being collected at your site, IBM Guardium S-TAP for IMS cannot report that event.
Parent topic: Reference information

Fields that are used for IMS policy pushdown

The following fields defined in the Guardium system Access Rule Definition panel are used by IBM Guardium S-TAP for IMS to create policies and rules. Use the following information as a guideline.

Table 1. Fields that are used for IMS Policy pushdown

Label	Hover text
Service Name	IMS names to which this rule applies (case sensitive)
Application User	INCLUDE/PSB or EXCLUDE/PSB
Database User	INCLUDE/USERID or EXCLUDE/USERID
Object	INCLUDE/read+update+delete+insert+data+image/DBNAME.SEGNAME or EXCLUDE/DBDNAME.SEGNAME

Service name/IMS name
: Required.
Must be 1 -- 8 characters.
Mixed case is allowed, and field is case sensitive.
Wildcard characters are not allowed.

Application user/PSB
: Must be 1 -- 8 characters.
All typed characters should be folded to uppercase.
Supports % as a wildcard character. % matches zero or more characters.
Note: If the keyword EXCLUDE is used, at least one INCLUDE must also be specified.

Database user/User ID
: Must be 1 -- 8 characters.
All typed characters should be folded to uppercase.
Supports % as a wildcard character. % matches zero or more characters.
Note: If the keyword EXCLUDE is used, at least one INCLUDE must also be specified.

Object/Target DB/Segment
: database_name must be 1 -- 8 characters.
segment_name must be 1 -- 8 characters.
wildcard_pattern supports % as a wildcard character. % matches zero or more characters.
All typed characters should be folded to uppercase.
Note: You must specify at least one INCLUDE with at least one DLI call type. DBD and segment must also be specified.

DLI Call Code
: Used to generate audit records for DLI calls that result in a non-blank status codes. Non-blank status codes can indicate that the DLI call failed or completed with a warning.
The following DLI status codes can be audited:

- FD
- FW
- GA
- GB
- GD
- GE
- GK
- L2
- LB
- LS
- NI
- UC
- US
- UX

You can specify one or more DLI status codes.
For more information about DLI status codes, see the About DLI status codes information in the IBM Knowledge Center.

Audit
: Used to limit the types of DLI calls to be audited.
NOHLVL causes audit information to be collected for only the target segment of a DLI Patch call (Command code C or D) instead of generating audit data for each segment of the hierarchical path. This can reduce the volume of audited data that is sent to, and stored by, the Guardium appliance in cases where the target segment concatenated key is sufficient for auditing purposes.

LTERM Filtering
: Must be 1 -- 8 characters.
All typed characters should be folded to uppercase.
Supports % as a wildcard character. % matches zero or more characters.
Note: If the keyword EXCLUDE is used, at least one INCLUDE must also be specified.

By default, auditing is considered for any DLI call that has a blank/null LTERM (for example, from a BMP or other region type that does not present IMS with an LTERM value). When an LTERM value or a group of LTERMs is specified, an option box is presented to enable you to turn off BLANK LTERM auditing. Turning off BLANK LTERM auditing does not affect the auditing of BMPs; any other region types without an LTERM value are excluded from auditing.

Filtering DLI calls from specific IMS Region types

You can filter out DLI calls from specific IMS Region types. DLI calls that originate from one or more of these region types can be excluded from auditing consideration:

- AER
- BMP
- CICS
- DBCTL
- IFP
- MPP
- ODB

In the Guardium interface, click the pencil icon alongside the Region Types to Exclude field to open a set of check-boxes that enable you to remove regions from auditing

Parent topic: Reference information

Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS

This section details the process of sizing the z/OS System Logger Log Streams. The z/OS System Logger Log Stream is used to transport audited DLI call data from the IMS control region or DLI/DBB batch jobs to the IBM® Guardium® S-TAP® for IMS agent (AUIAxxxx address space) where it is reformatted to a PROTOBUF protocol and sent to the target Guardium appliance.

- **Calculating the Optimal Log Stream Size**
  Filtering by using the IMS POLICY from the Guardium appliance occurs in the IMS Control region, therefore only DLI calls that are to be audited are written to the log stream(s).
- **Considerations**
  There are several variables that must be considered when sizing the log stream(s), including:
- **Using IBM Documentation**
  The System Logger Performance and Tuning section of the System Programmer's Guide to: z/OS System Logger provides a detailed description of the processes that are needed to tune the System Logger for use with IBM Guardium S-TAP for IMS and other products.
- **Pertinent Report Fields**
  Some key fields provided in the System Logger Activity Report (IXGRPT1) are the BYT WRITTN TO INTERIM STORAGE, BYT WRITTN TO DASD, and STRUC FULL.
- **Additional Resources**
  IBM provides a spreadsheet utility to assist in the analysis of the log stream SMF88 data and provide suggestions on how to define the log stream for more efficient use in your environment.

Parent topic: Reference information

Calculating the Optimal Log Stream Size

Filtering by using the IMS POLICY from the Guardium appliance occurs in the IMS Control region, therefore only DLI calls that are to be audited are written to the log stream(s).

For most users, the size of the log stream that is provided with the LS_SIZE parameter of the AUILSTR2/3 log stream definition member (LS_SIZE(100)) is appropriate to use when auditing accesses to sensitive data or when auditing DLI calls performed by a group, or groups, of users who have access to all databases for diagnostic purposes.

There might be instances where an LS_SIZE parameter value of 13500 (LS_SIZE(13500)) might be used, such as:

- during product testing, or
- when the number of audited DLI calls exceed twenty-five thousand DLI calls per second, or
- when the audited DLI calls include large concatenated key or large segment fields, which can occur when the IMS POLICY includes the `+DATA` keyword in the TARGET/DB INCLUDE filter statement

Note: Log stream sizing can be an iterative process. When attempting to audit many DLI calls, the CPU, memory, and disk storage capacity of the Guardium appliance should be considered.

Parent topic: Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS

Considerations

There are several variables that must be considered when sizing the log stream(s), including:

- the number of IXGWRITEs that are performed every second
- the average number of bytes written, or average buffer size written with each IXGWRITE calls
- the rate that the data is offloaded from the log stream
- the number/rate of IXGDELETEs that are performed

The average number of IXGWRITEs that are performed and the average number of bytes/average buffer size is determined by the volume of audited DLI calls and the size of the DLI call event data that is being captured.

IBM® Guardium® S-TAP® for IMS uses a set of 35K buffers to hold the audited DLI call data. Each buffer is written to the log stream when it fills to capacity, or every five seconds. The time interval is used to ensure that audited DLI call data is sent to the Guardium appliance in a timely manner. Therefore, the frequency of IXGWRITEs can vary greatly depending on the IMS Policy and databases that are being accessed.

The log stream offload process IBM Guardium S-TAP for IMSis performed by the agent address space (AUIAxxxx). The agent address space constantly polls the log stream (once per second) looking for new data to process. When new data is found, the data is read by using the IXGBRWSE call. The data is formatted into a PROTOBUF protocol and sent to the Guardium appliance by using TCP/IP. The IBM Guardium S-TAP for IMS agent will continually read and process log stream data until no new data exists, at which time, polling every second will reoccur.

The log stream data is deleted by using the IXGDELETE call after every three blocks of data are successfully read and sent to the Guardium appliance. This ensures that audited data is not lost in the event of a communication loss between the IBM Guardium S-TAP for IMS agent and the Guardium appliance.

Parent topic: Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS

Using IBM Documentation

The System Logger Performance and Tuning section of the System Programmer's Guide to: z/OS System Logger provides a detailed description of the processes that are needed to tune the System Logger for use with IBM® Guardium® S-TAP® for IMS and other products.

You can perform an analysis of the performance and efficiency of the initial log stream size by running program IBM program IXGRPT1 and JCL IXGRPT2 found in 'SYS1.PROCLIB'. This program uses the SMF88 records to help with log stream capacity planning.

SMF88 records can be collected by z/OS by providing the 88 value in the SMPRM parmlib member prior to a system IPL, or by using the z/OS command, "SET SMF=xx" (where xx is the suffix of the parmlib member).

Example:

```
SYS(TYPE(30,70:79,88,89,100,101,110)),
```

The IXGRPT1 utility will assemble sub-routine IXGRA1 and compile and link program IXGRPT1, which can be used to extract SMP88 records in preparation for analysis.

The IXGRPT2 JCL can be used to produce other SMP88/log stream reports.

Parent topic: Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS

Pertinent Report Fields

Some key fields provided in the System Logger Activity Report (IXGRPT1) are the BYT WRITTN TO INTERIM STORAGE, BYT WRITTN TO DASD, and STRUC FULL.

BYT WRITTN TO INTERIM STORAGE

The BYT WRITTN TO INTERIM STORAGE value (bytes written to interim storage) indicates the amount of data being written to the log stream during the SMP interval. This value can provide insight as to the volume of data being written to the log stream.

BYT WRITTN TO DASD

The BYT WRITTN to DASD value (bytes written to DASD offload data sets) indicates the number of bytes that were written to the DASD offload/overflow VSAM data sets.

This number indicates that the interim storage filled up, and in order to retain the data, a set of VSAM files are being used as overflow buffers. This number can rise and fall during the day as the volume of audited DLI calls increase and decrease.

Some use of the overflow VSAM files can be acceptable because spikes in audited DLI call data can certainly be expected due to the nature of IMS POLICY filtering. However, constant or extensive use of the VSAM overflow files indicate that the log stream should be sized larger.

STRC FULL

The STRC FULL (Structure Full) value indicates the number of times that the capacity of the CF structure was filled up without an offload occurring. This number should be zero in a properly sized log stream. Structure such as this can indicate that the volume of data written exceeds the offload capability of the IMS STAP agent to read, process, and delete audited data, and a larger structure size should be considered.

An abundance of Structure Full conditions will result in a degradation of performance when collecting audited DLI call data, and if not rectified, might result in data loss. This condition might result in IXGWRITE 0866 errors being issued in the IMS Control region address space.

Parent topic: Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS

Additional Resources

IBM provides a spreadsheet utility to assist in the analysis of the log stream SMF88 data and provide suggestions on how to define the log stream for more efficient use in your environment.

You can access the spreadsheet utility with the following link: ftp://www.redbooks.ibm.com/redbooks/SG246898. Read the disclaimer.txt file before using the tool.

Parent topic: Sizing the z/OS System Logger Log Stream for IBM Guardium S-TAP for IMS

Echoed XML statement definitions

IBM® Guardium® S-TAP® for IMS echoes the XML statements that are produced by the Guardium appliance to represent an Audit Policy. These statements are issued to a physical data set, agent AUILOG DD, or both, as determined by the XML_ECHO_DATASET and XML_ECHO_AUILOG parameters. This topic provides definitions of all XML statements that could be echoed from the appliance by the S-TAP.

XML convention

Start of tag data

=<*tag_name*>
End of tag data
=</*tag_name*>
Null/empty tag
=<*tag_name*/>

See Sample XML file for an example of the XML representation of a valid policy.

IMS-specific statements

Table 1. IMS-specific XML statements

XML statement	Definition
<install-info>	Beginning of relevant policy information.
<artifacts>	Start of IMS definitions.
<ims>	Start of individual IMS-specific information.
<name>	Name of IMS as specified in the Guardium appliance policy.
<agent>	Name of the agent to which IMS is connected.
<description>	Appliance IMS description text.
<version>	Currently a value of zero (0).
<plexname>	Not populated.
<recons>	Start of the IMS-specific RECON data set list.
<recon seq="1">	RECON1 data set name. DSN terminated by </recon>.
<recon seq="2">	RECON2 data set name. DSN terminated by </recon>.
<recon seq="3">	RECON3 data set name. DSN terminated by </recon>.
<reslibs>	Start of IMS-specific RESLIB data sets.
<reslib seq="1">	RESLIB 1 in IMS STEPLIB concatenation. DSN terminated by </reslib>.

Log-specific statements

Table 2. Log-specific XML statements

XML statement	Definition
<dbdlibs/>	Not populated.
<psblibs/>	Not populated.
<thresholds-050i>	Start of message AUII050I message frequency parameters.
<max-count>	Number of DLI calls needed to prompt message AUII050I.
<max-time>	Max time interval (HHMM) between AUII050I messages.
<audit-levels>	Start of IMS Logger and SMF auditing criteria.
<collector name="ims">	Start of IMS Logger auditing criteria. Terminated by </collector>.
<audit-level>	Start of audit level criteria.
<signon-signoff value="true"/>	Audit IMS user sign-ons and sign-offs.
<signon-signoff value="false"/>	Do not audit IMS user sign-ons and sign-offs.
<start-stop value="true"/>	Audit IMS Control Region starts and stops.
<start-stop value="false"/>	Do not audit IMS Control Region starts and stops.
<db-open-close value "true"/>	Audit DBD Opens and Closes.
<db-open-close value "false"/>	Do not audit DBD Opens and Closes.
<dbd-psb value="true/"	Audit DBD/PSB/Dump/Start/Stop/Lock/Unlock
<dbd-psb value="false/"	Audit DBD/PSB/Dump/Start/Stop/Lock/Unlock

SMF-specific statements

Table 3. SMF-specific XML statements

XML statement	Definition
<collector name="smf">	Start of SMF auditing criteria. Terminated by </collector>.
<audit-level>	Start of audit-level criteria.
<read value="true"/>	Audit data sets when they are opened with READ intent.
<read value="false"/>	Do not audit data sets when they are opened with READ intent.
<update value="true"/>	Audit data sets when opened with UPDATE intent.
<update value="false"/>	Do not audit data sets when opened with UPDATE intent.
<delete value="true"/>	Audit data set DELETEs.
<delete value="false"/>	Do not audit data set DELETEs.
<create value="true"/>	Audit data set CREATEs.
<create value="false"/>	Do not audit data set CREATEs.
<alter value="true"/>	Audit VSAM data set ALTERs.
<alter value="false"/>	Do not audit VSAM data set ALTERs.
<racf-violations value "true"/>	Audit RACF security violations against data sets.
<racf-violations value "false"/>	Do not audit RACF security violations against data sets.

Policy-specific statements

Table 4. Policy-specific XML statements

XML statement	Definition

XML statement	Definition
<policies>	Start of policy information.
<collection-profile>	Displays the rules defined to the policy. The collection profile policy name appears in the collection-specific statement <collection> for a given <ims>.
<name>	Policy name. Naming convention is: *policy_IMS_name*.
<description>	Concatenation of descriptions of all policies pushed to the appliance.
<rules>	Start of individual policy rules.
<rule>	Start of rule instance.
<active>	Always a value of true.
<filters>	Start of PSB/USERID/LTERM INCLUDES/EXCLUDES within the rule.
<psb-filter>	PSB instance.
<name>	Name of PSB to be audited or ignored.
<type>	Value will be INCLUDE (audit) or EXCLUDE (ignore).
<lterm-filter>	LTERM instance.
<name>	LTERM to be audited or ignored.
<type>	Value will be INCLUDE (audit) or EXCLUDE (ignore).

Database/segment-specific statements

Table 5. Database/segment-specific XML statements

XML statement	Definition
<targets>	Start of DBD/SEGMENT instances within the rule.
<segment-target>	Start of list of databases/segments to be INCLUDED/EXCLUDED.
<type>	Value will be INCLUDE (audit) or EXCLUDE (ignore).
<database-name>	Database to be audited or ignored.
<segment-name>	Segment to be audited or ignored.
<audit-get>	INCLUDE DLI GET calls.
<audit-insert>	INCLUDE DLI INSERT calls.
<audit-update>	INCLUDE DLI UPDATE (REPL) calls.
<audit-delete>	INCLUDE DLI DELETE (DLET) calls.
<capture-before-image>	INCLUDE link between DLI GH and DLI REPL calls.
<capture-segment-data>	INCLUDE segment data when segment is audited.
<hlvl-filter enabled="false">	Do not report hierarchical parent segment during DLI command calls.
<excluded-regions>	Do not audit DLI calls from these region types.

Collection-specific statements

Table 6. Collection-specific XML statements

XML statement	Definition
<collections>	A grouping of the individual <collection> XML tags.
<ims>	IMS name connection to the collection.
<agent-name>	Agent name connection to the collection.
<name>	IMS name connection to the collection.
<collection-profile>	For each agent name and IMS name, IBM Guardium S-TAP for IMS establishes a connection to the collection profile.
<name>	Constructed name of the policy (*policy_IMS_NAME*).
<dli-status-codes>	Two-character DLI status codes to be audited. Terminated by FF value.

Quarantine information

Quarantine XML is only sent from the appliance when the quarantine is triggered by audited events that are sent to the appliance by the agent, and the quarantine is deemed to be in effect. This causes AI status codes (error opening database) to be returned to the application program in the DLI Status code PCB field (DBPCBSTC), and message AUIJ252W to appear in the IMS region or batch job.

Quarantine only works with full-function DLI calls because the AUI hook for Fast-Path occurs after the DLI call has completed. (The DLI call cannot be preempted.)

Table 7. Quarantine-specific XML statements

XML statement	Definition
<quarantine-lists>	Start of quarantine section.
<quarantine-list agent-name="*xxxxxxxx*" ims-name="*yyyyyyyy*"> >	Agent and IMS name are affected.
<quarantine-item>	Start of quarantine details.
<start-ts>yyyy-mm-dd-hh.mm.ss.000000	Quarantine start date/time.
<end-ts>yyyy-mm-dd-hh.mm.ss.000000	Quarantine end date/time.
<user-id>	User ID to be quarantined.

- **Sample XML file**
  This is an example of a valid audit policy.
- **Additional causes of AUIA060W**
  Warning message AUIA060W can appear if the data set location is incorrect. Review these additional possible causes of the message if the explanation and recommendation provided by AUIA060W do not resolve the warning.

Parent topic: Reference information

Sample XML file

This is an example of a valid audit policy.

```
<install-info>
  <artifacts>
    <ims>
      <name>IMSV14AH</name>
      <agent>AUI15A</agent>
      <description>IMS V14 Test IEACRX AUI10A27</description>
      <version>0</version>
      <plexname></plexname>
      <recons>
        <recon seq="1">IMSEA1.RECON1</recon>
        <recon seq="2">IMSEA1.RECON2</recon>
        <recon seq="3">IMSEA1.RECON3</recon>
      </recons>
      <reslibs>
        <reslib seq="1">IMSEA1.SDFSRESL</reslib>
      </reslibs>
      <dbdlibs/>
      <psblibs/>
      <thresholds-050i>
        <max-count>1K</max-count>
        <max-time>0015</max-time>
      </thresholds-050i>
      <audit-levels>
        <collector name="ims">
          <audit-level>
            <signon-signoff value="true"/>
            <start-stop value="true"/>
            <db-open-close value="true"/>
            <dbd-psb value="true"/>
          </audit-level>
        </collector>
        <collector name="smf">
          <audit-level>
            <read value="true"/>
            <update value="true"/>
            <delete value="true"/>
            <create value="true"/>
            <alter value="true"/>
            <racf-violations value="true"/>
          </audit-level>
        </collector>
      </audit-levels>
    </ims>
  </artifacts>
  <policies>
    <collection-profile>
      <name>policy_IMSV14AH</name>
      <description>---: Log Full Details With Values,Auv - Event All,IEA1_ALL_ST_AH</description>
      <rules>
        <rule>
          <active>true</active>
          <filters/>
          <targets>
            <segment-target>
              <type>include</type>
              <database-name>%</database-name>
              <segment-name>%</segment-name>
              <audit-get>true</audit-get>
              <audit-insert>true</audit-insert>
              <audit-update>true</audit-update>
              <audit-delete>true</audit-delete>
              <capture-before-image>false</capture-before-image>
              <capture-segment-data>true</capture-segment-data>
            </segment-target>
          </targets>
          <audit/>
          <excluded-regions></excluded-regions>
        </rule>
      </rules>
    </collection-profile>
  </policies>
  <collections>
    <collection>
      <ims>
        <agent-name>AUI15A</agent-name>
        <name>IMSV14AH</name>
      </ims>
      <collection-profile>
        <name>policy_IMSV14AH</name>
      </collection-profile>
      <dli-status-codes>FDFWGAGBGDGEGKL2LBLSNIUCUSUXFFFF</dli-status-codes>
    </collection>
  </collections>
  <quarantine-lists/>
</install-info>
```

Parent topic: Echoed XML statement definitions

Additional causes of AUIA060W

Warning message AUIA060W can appear if the data set location is incorrect. Review these additional possible causes of the message if the explanation and recommendation provided by AUIA060W do not resolve the warning.

Data set: <LOCATION> in use

Explanation
: An attempt to dynamically allocate the data set failed because the data set was in use by another process. This warning might be temporary. The agent retries the data set 6 times in 3 seconds before skipping the policy XML echoing.

Response
: If this message occurs several times without successful policy XML echoes, check to see that any running user report program is using the data set correctly or whether a TSO user might be editing the data set.

A dynamic allocation error occurred. Data set <LOCATION>, info code: <info-code>, error code: <error-code>.

Explanation
: An attempt to dynamically allocate the data set failed. The specified information and error codes reflect the return and reason codes from the z/OS dynamic allocation services.

Response
: Use the info code and error code to determine the cause of the dynamic allocation failure by referring to the *z/OS MVS Programming: Authorized Assembler Services Guide* in the IBM Knowledge Center. Correct the error and restart the agent.

Catalog Search Interface: error RC = <rc>, RSN = <rsn>.

Explanation
: Using the z/OS Catalog Search Interface routine, the agent attempted to analyze whether the data set is a Generation Data Group (GDG) data set or a non-VSAM data set. An error occurred while calling the routine.

Response
: Consult the *Return Codes for General Purpose Register 15* section of the *IBM Catalog Search Interface User's Guide* in the IBM Knowledge Center. Contact IBM Support if additional assistance is needed.

Data set "<LOCATION>" could not be deleted, info code: <code>, error code <code>.

Explanation
: An attempt was made to delete and reallocate a non-VSAM non-GDG data set in the catalog.

Response
: Ensure that the agent task has RACF (or other security product) authority to delete a data set that contains a high-level qualifier. Attempt to correct the security problem and restart the agent. If the error persists, contact IBM Support and provide the info and error codes.

XML echo data set <LOCATION> is of an unsupported type

Explanation
: Only non-VSAM and GDG base data sets are supported.

Response
: Ensure that the data set type is either a non-VSAM data set or a Generation Data Group. Restart the agent.

Parent topic: Echoed XML statement definitions

Troubleshooting

Use the following topics to diagnose and correct problems that you experience with IBM Guardium S-TAP for IMS.

- **Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS**

Parent topic: IBM Security Guardium S-TAP for IMS on z/OS

Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

This information documents the messages and error codes issued by Security Guardium S-TAP for IMS. Messages are presented in ascending alphabetical and numerical order.

Note: To set a z/OS message alert for messages that begin with AUII, or messages AUIJ250I and AUIJ252W, use single-dash formatting between the message number and message text. For all other messages, use a double-dash. For example:

AUIT031I--Starting the command listener thread
: Format most message alerts with double-dashes between the message number and message text.

AUII056I - ZIIP PROCESSING ENABLED FOR IMS STAP
: Format message alerts for AUII*, AUIJ250I, and AUIJ252W with a single dash between the message number and message text.

- **Error messages and codes: AUIAxxxx**
- **Error messages and codes: AUIBxxxx**
- **Error messages and codes: AUIFxxxx**
- **Error messages and codes: AUIGxxxx**
- **Error messages and codes: AUIIxxxx**
- **Error messages and codes: AUIJxxxx**

- **Error messages and codes: AUILxxxx**
- **Error messages and codes: AUIPxxxx**
- **Error messages and codes: AUIRxxxx**
- **Error messages and codes: AUITxxxx**
- **Error messages and codes: AUIUxxxx**
- **Error messages and codes: AUIXxxxx**
- **Error messages and codes: AUIYxxxx**
- **Error messages and codes: AUIZxxxx**

Parent topic: Troubleshooting

Error messages and codes: AUIAxxxx

The following information is about error messages and codes that begin with AUIA.

- **AUIA003E**
  Address Space *<name>* failed to start successfully on *<LPAR name>*.
- **AUIA004E**
  Address Space *<name> (<job number>)* failed to stop successfully on *<LPAR name>* within the timeout period and was abandoned.
- **AUIA005I**
  Starting address space *<name>* on *<LPAR name>*.
- **AUIA006I**
  Address Space *<name> (<job number>)* is online on *<LPAR name>*.
- **AUIA007I**
  Stopping address space *<name> (<job number>)* on *<LPAR name>*.
- **AUIA008I**
  Address Space *<name> (<job number>)* on *<LPAR name>* is offline.
- **AUIA009E**
  Address space *<name>* is not active.
- **AUIA010E**
  Address Space *<name>* is already active.
- **AUIA021I**
  MODIFY command *<command text>* sent to Address Space *<name>*.
- **AUIA022I**
  <Collector name> collector is disabled: interval is set to *<value>*.
- **AUIA023I**
  <Collector name> collector is disabled: proc name for the collector address space has not been specified in the configuration.
- **AUIA024I**
  <Collector name> collector is disabled: not configured.
- **AUIA027E**
  Abend occurred while validating *<log stream>*. Abend code = *<code>*, RSN = *<reason>*.
- **AUIA028S**
  Agent *agent-name* on *PLEX name* for S-TAP version *S-TAP version* is already online. *(ADS_SHM_ID=<Memory Segment ID>)*
- **AUIA029I**
  collector collector is disabled: no Audit IMS Log Events are selected for IMS source *IMS*.
- **AUIA030I**
  collector collector started successfully.
- **AUIA031I**
  collector collector stopped successfully.
- **AUIA033I**
  (GDM) Attempting to establish link with the appliance.
- **AUIA034S**
  (GDM) An attempt to establish the link to the appliance failed.
- **AUIA035W**
  (GDM) Link failed over to a secondary appliance. [host=*host*, port=*port*]
- **AUIA036I**
  (GDM) Link to primary appliance established. [host=*host*, port=*port*]
- **AUIA037I**
  (GDM) Link to primary appliance restored. [host=*host*, port=*port*]
- **AUIA038S**
  (GDM) Link to the appliance lost.
- **AUIA041I**
  Guardium policy processing failed due to prior errors.
- **AUIA042W**
  The Guardium policy is not applicable.
- **AUIA043I**
  The Guardium policy reader thread started.
- **AUIA044I**
  The Guardium policy reader thread is terminating.
- **AUIA045I**
  The guardium policy reader thread is terminating due to prior errors.
- **AUIA048I**
  auiu_taskname is configured to start only on *lpar-name*.
- **AUIA049W**
  auiu_task_name is configured to not start on *lpar_name* but will be started on *lpar_name* because *aui_agent_name* runs on *lpar_name*
- **AUIA050W**
  auiu_task_name is configured to not start on *lpar_name* but no such system exists.
- **AUIA051I**
  auiu_task_name is configured to not start on *lpar_name* and will not be started on *lpar_name*.

- **AUIA052I**
  Discovered <plex-name> system <system-name>.
- **AUIA053I**
  Agent configuration option *<option>* has been updated to *<value>*.
- **AUIA054I**
  Agent configuration option *<option>* is set to *<value>*.
- **AUIA055I**
  The agent is waiting for start-up information from the appliance.
- **AUIA056I**
  Starting the agent collectors.
- **AUIA057I**
  Issuing request to capture agent status.
- **AUIA058I**
  Request to capture agent status has completed successfully.
- **AUIA059I**
  Policy XMl echo
- **AUIA060W**
  Policy XML echo to data set skipped: *<MESSAGE> <LOCATION>*
- **AUIA061I**
  Policy XML echo to data set *<LOCATION>* completed.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIA003E Address Space *<name>* failed to start successfully on *<LPAR name>*.

Explanation

An attempt by the agent to start the named support address space has failed.

User response

Check the named address space logs to identify why it was not able to start. In most cases, this occurs if an address space with that name is already online, there was a JCL error, or there was an issue resolving the loopback address host name. If further assistance is required, contact IBM Software Support.

Parent topic: Error messages and codes: AUIAxxxx

AUIA004E Address Space *<name> (<job number>)* failed to stop successfully on *<LPAR name>* within the timeout period and was abandoned.

Explanation

The specified address space did not stop within the time out period and was consequently abandoned by the master address space.

User response

Check the named address space logs to identify why it did not stop. If further assistance is needed, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIAxxxx

AUIA005I Starting address space *<name>* on *<LPAR name>*.

Explanation

The agent has automatically started the support address named.

User response

This is an informational message only.
Parent topic: Error messages and codes: AUIAxxxx

AUIA006I Address Space *<name> (<job number>)* is online on *<LPAR name>*.

Explanation

The agent has successfully started the support address space named.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA007I Stopping address space *<name> (<job number>)* on *<LPAR name>*.

Explanation

The agent has automatically stopped the support address space named.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA008I Address Space *<name> (<job number>)* on *<LPAR name>* is offline.

Explanation

The named address space has successfully stopped.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA009E Address space *<name>* is not active.

Explanation

The specified address space that the master address space was attempting to control is not online.

User response

Correct and retry.

Parent topic: Error messages and codes: AUIAxxxx

AUIA010E Address Space *<name>* is already active.

Explanation

This message indicates that the address space with the specified name is active already and was expected to be. This message occurs when starting the BATCH (or SMF) collector if they are already running.

User response

Verify that the address space is already running. If the address space is not online and the message occurs, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIAxxxx

AUIA021I MODIFY command *<command text>* sent to Address Space *<name>*.

Explanation

The MODIFY command *<command text>* sent to address space named.

User response

No action is required.

Parent topic: Error messages and codes: AUIAxxxx

AUIA022I *<Collector name>* collector is disabled: interval is set to *<value>*.

Explanation

Named collector is disabled because the interval value is less than or equal to zero.

User response

If this was not intentional, fix the interval value and restart the agent address space.

Parent topic: Error messages and codes: AUIAxxxx

AUIA023I *<Collector name>* collector is disabled: proc name for the collector address space has not been specified in the configuration.

Explanation

The specified collector is disabled because the procedure name for the collector address space has not been specified in the configuration.

User response

To enable this collector, specify the procedure name for collector address space. If the procedure name is specified and this message still occurs, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIAxxxx

AUIA024I *<Collector name>* collector is disabled: not configured.

Explanation

The specified collector is disabled because it has not been configured.

User response

To enable this collector, configure it using the Guardium user interface. If the specified collector is configured and the message still occurs, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIAxxxx

AUIA027E Abend occurred while validating *<log stream>*. Abend code = *<code>*, RSN = *<reason>*.

Explanation

The Log Stream *log stream* validation failed with abend code *code* and reason code *reason*.

User response

Contact IBM Software Support.
Parent topic: Error messages and codes: AUIAxxxx

AUIA028S Agent *agent-name* on *PLEX name* for S-TAP version *S-TAP version* is already online. *(ADS_SHM_ID=<Memory Segment ID>)*

Explanation

The specified agent is already online. Agent names must be unique per sysplex.

User response

Change the *agent-name* and restart the agent, or shut down the other agent.
Parent topic: Error messages and codes: AUIAxxxx

AUIA029I *collector* collector is disabled: no Audit IMS Log Events are selected for IMS source *IMS*.

Explanation

An Audit IMS Log Event must be selected for the IMS source *IMS* for the collector to be enabled.

User response

To enable the collector, select an Audit IMS Log Event for the IMS source.
Parent topic: Error messages and codes: AUIAxxxx

AUIA030I *collector* collector started successfully.

Explanation

The specified collector started.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA031I *collector* collector stopped successfully.

Explanation

The specified collector stopped.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA033I (GDM) Attempting to establish link with the appliance.

Explanation

The agent is attempting to establish a connection to one of the appliances specified in the agent configuration.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA034S (GDM) An attempt to establish the link to the appliance failed.

Explanation

The agent could not establish a connection to any of the appliances specified in the configuration.

User response

Contact your network administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIAxxxx

AUIA035W (GDM) Link failed over to a secondary appliance. [host=*host*, port=*port*]

Explanation

The agent lost connection to the primary appliance and switched to the specified secondary appliance.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA036I (GDM) Link to primary appliance established. [host=*host*, port=*port*]

Explanation

The agent has connected to the specified primary appliance.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA037I (GDM) Link to primary appliance restored. [host=*host*, port=*port*]

Explanation

The agent has reconnected to the specified primary appliance.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA038S (GDM) Link to the appliance lost.

Explanation

All attempts to connect to the appliances specified in the configuration have failed.

System action

Any new policies defined in the appliance will not be pushed down to the IBM® Guardium® S-TAP® for IMS agent.

User response

Verify network connectivity to the appliance. Contact your network administrator or IBM Software Support.
Parent topic: Error messages and codes: AUIAxxxx

AUIA041I Guardium® policy processing failed due to prior errors.

Explanation

The Guardium policies could not be processed.

User response

Check the log for previous errors.
Parent topic: Error messages and codes: AUIAxxxx

AUIA042W The Guardium® policy is not applicable.

Explanation

One or more of the policy rules cannot be used by the current agent.

User response

Check the log for previous errors to determine why the policy is not applicable and fix the policy definition.
Parent topic: Error messages and codes: AUIAxxxx

AUIA043I The Guardium® policy reader thread started.

Explanation

The Guardium policy reader thread started.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA044I The Guardium® policy reader thread is terminating.

Explanation

The Guardium policy reader thread is stopping.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA045I The guardium policy reader thread is terminating due to prior errors.

Explanation

The policy reader thread is stopping due to previously reported errors.

User response

Check the previously issued messages to determine why the policy reader is terminating.
Parent topic: Error messages and codes: AUIAxxxx

AUIA048I *auiu_taskname* is configured to start only on *lpar-name*.

Explanation

The configuration file pointed to by the AUICONFG DD statement contains an AUIU_EXCLUDE_LPAR statement that has the *ALL parameter supplied as the excluded LPAR name.

System action

The AUIUSTC task is scheduled only on the home LPAR where the agent is running.

User response

To schedule the AUIUSTC task for another LPAR, remove or correct the AUIU_EXCLUDE_LPAR statement.
Parent topic: Error messages and codes: AUIAxxxx

AUIA049W *auiu_task_name* is configured to not start on *lpar_name* but will be started on *lpar_name* because *aui_agent_name* runs on *lpar_name*

Explanation

The AUIU_EXCLUDE_LPAR configuration parameter, found in the AUICONFG SAMPLIB member, was used in an attempt to prevent the AUIU task from executing on the LPAR named.

System action

The request to exclude this LPAR from AUIU processing is ignored because the specified LPAR is also where the agent is executing.

User response

Remove the LPAR name from the AUICONFG samplib member's AUIU_EXCLUDE_LPAR parameter. The change will be implemented at the next restart of the agent.
Parent topic: Error messages and codes: AUIAxxxx

AUIA050W *auiu_task_name* is configured to not start on *lpar_name* but no such system exists.

Explanation

The specified *lpar_name* has been included as part of the LPARS that are specified in the AUIU_EXCLUDE_LPAR configuration keyword. The specified *lpar_name* was not found in the list of members of either the SYSJES or *lpar_name* XCF groups.

System action

Processing continues.

User response

This message might indicate that the lpar_name is not available or that there is an error in the specified lpar_name.
Parent topic: Error messages and codes: AUIAxxxx

AUIA051I *auiu_task_name* is configured to not start on *lpar_name* and will not be started on *lpar_name*.

Explanation

The AUIU_EXCLUDE_LPAR configuration, parameter found in the AUICONFG SAMPLIB member, was used in an attempt to prevent the AUIU task from executing on the specified LPAR.

System action

An instance of the AUIU task is not routed to the excluded LPAR.

User response

None.
Parent topic: Error messages and codes: AUIAxxxx

AUIA052I Discovered <plex-name> system <system-name>.

Explanation

This LPAR name was found as a member of the XCF group when performing a z/OS IXCQUERY on the PLEXNAME of SYSJES XCF GROUPS.

System action

Processing continues

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA053I Agent configuration option <*option*> has been updated to <*value*>.

Explanation

This message indicates that command such as: /f AUIASTC,SET CONFIG <*option*> ON/OFF processed successfully.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA054I Agent configuration option <*option*> is set to <*value*>.

Explanation

This message indicates that command such as: /f AUIASTC,GET CONFIG <*option*> processed successfully.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA055I The agent is waiting for start-up information from the appliance.

Explanation

The agent has determined that there is no checkpoint information available for this agent in E/CSA, and is awaiting this data to be sent from the appliance.

System action

The agent waits up to 30 seconds for the checkpoint information, and if none is received, processing continues by using default checkpoint values, such as current blocks from the z/OS log-streams, and SMF and SLDS data sets that were created no earlier than the previous day.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA056I Starting the agent collectors.

Explanation

The agent is starting the auditing threads.

System action

The agent starts the DLIO/DLIB/AUIL/AUIF auditing threads.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA057I Issuing request to capture agent status.

Explanation

A command, such as /f AUIASTC,STATUS, has been issued for processing.

User response

No action is required.

Parent topic: Error messages and codes: AUIAxxxx

AUIA058I Request to capture agent status has completed successfully.

Explanation

A command, such as /f AUIASTC,STATUS has processed successfully.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

AUIA059I Policy XMl echo

Explanation

If the XML_ECHO_AUILOG(Y) keyword exists in the AUICONFG, this message will be followed by the echo of all active XML policies on the AUILOG.

System action

As an example, the first three lines of the echo appear as follows:

```
<?xml version="1.0" encoding="IBM-1047" standalone="yes"?>
<!-- 2019-03-25-13.35.57.354196 -->
<install-info>
```

User response

For more information, see Echoed XML statement definitions.
Parent topic: Error messages and codes: AUIAxxxx

AUIA060W Policy XML echo to data set skipped: *<MESSAGE> <LOCATION>*

Explanation

The XML of the policy that was installed from the Security Guardium® system was not echoed to the specified location due to the specified message. If the &Data_Set_Name parameter contains z/OS system variables, <LOCATION> reflects the data set name after symbol substitution has been done.

<MESSAGE> <LOCATION> can be:

- The installed policy has not been changed. The echo is skipped if the newly installed policy has not changed since it was last installed.
- The data set location is not valid. Incorrect use of a system symbol in the &Data_Set_Name parameter can invalidate the location. Additional requirements:
  - The data set name must not exceed 44 characters.
  - The segment length must be greater than zero and less than or equal to 8.
  - The first character in each segment must be a letter (A – Z), #, @, $, or hyphen.

System action

Processing continues.

User response

Correct the &Data_Set_Name parameter and restart the agent. If the error persists, see Additional causes of AUIA060W .
Parent topic: Error messages and codes: AUIAxxxx

AUIA061I Policy XML echo to data set *<LOCATION>* completed.

Explanation

The agent has completed the XML echo of all active policies that were installed from the Security Guardium® system. *<LOCATION>* is the data set name specified by the &Data_Set_name parameter of the XML_ECHO_DATASET keyword.

System action

The data set name reflects the z/OS system variable substitution and the Generation Data Group extension if either exists in the &Data_Set_name parameter.

User response

No action is required.
Parent topic: Error messages and codes: AUIAxxxx

Error messages and codes: AUIBxxxx

The following information is about error messages and codes that begin with AUIB.

- **AUIB300I**
  CONNECTION TO z/OS® SYSTEM *type* LOG STREAM WAS SUCCESSFUL - LOG STREAM NAME: *log_stream_name*, LOG STREAM TYPE: *XCF-BASED|DASD_ONLY*, CHECKPOINT VALUE: *check_point_value*, CHECKPOINT PTR: *address_of_checkpoint*

- **AUIB302I**
  DRAIN REQUEST FOR *type* LOG STREAM HAS COMPLETED. LOG STREAM: *name*.
- **AUIB305I**
  DRAIN COMPLETE FOR LOG STREAM *log-stream name*
- **AUIB306E**
  INVALID RECORD FOUND IN *log-stream* LOG STREAM -RECORD IMAGE SNAPPED TO AUI$NAP DD
- **AUIB700I**
  type: *LOGSTREAM CHECKPOINT INFORMATION* - LOG STREAM NAME: *log-stream-name* - CHECKPOINT VALUE: *check_point_value* - LAST UPDATED (UTC): *date_time*

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIB300I CONNECTION TO z/OS® SYSTEM *type* LOG STREAM WAS SUCCESSFUL - LOG STREAM NAME: *log_stream_name*, LOG STREAM TYPE: *XCF-BASED|DASD_ONLY*, CHECKPOINT VALUE: *check_point_value*, CHECKPOINT PTR: *address_of_checkpoint*

Explanation

The connection to the log-stream name (*log_stream_name*) configured to process *log_stream_type* events completed successfully.

System action

Processing continues

User response

No action is required.
Parent topic: Error messages and codes: AUIBxxxx

AUIB302I DRAIN REQUEST FOR *type* LOG STREAM HAS COMPLETED. LOG STREAM: *name*.

Explanation

A DRAIN request, which reads all data from the z/OS® log stream, has completed.

System action

The AUIASTC tasks prepare to terminate.

User response

No action is required.
Parent topic: Error messages and codes: AUIBxxxx

AUIB305I DRAIN COMPLETE FOR LOG STREAM *log-stream name*

Explanation

A DRAIN request used to flush read all existing events from the log-stream-name indicated has completed successfully

System action

The log-stream reader thread will start the termination phase.

User response

No action is required.
Parent topic: Error messages and codes: AUIBxxxx

AUIB306E INVALID RECORD FOUND IN *log-stream* LOG STREAM -RECORD IMAGE SNAPPED TO AUI$NAP DD

Explanation

When reading DLI call audit records from the z/OS System log stream, a malformed audit record was encountered or the version of the audit record was not recognized.

System action

Processing continues after writing a SNAP/DUMP of the offending record to the AUI$NAP DD.

User response

First, verify that the S-TAP version that is running in the IMS Control Region and/or Batch Region is the same as is running in the agent. If adjusting the version does not resolve the issue, forward the AUI$NAP output to IBM Software Support.
Parent topic: Error messages and codes: AUIBxxxx

AUIB700I type: *LOGSTREAM CHECKPOINT INFORMATION* - LOG STREAM NAME: *log-stream-name* - CHECKPOINT VALUE: *check_point_value* - LAST UPDATED (UTC): *date_time*

Explanation

This message provides the highest block ID for the log stream. This is used as the starting checkpoint for processing data from this log stream.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIBxxxx

Error messages and codes: AUIFxxxx

The following information is about error messages and codes that begin with AUIF.

- **AUIF002I**
  SMF log reader interval set to *<n>* minutes.
- **AUIF003E**
  Command *<command>* failed; interval value must be between *<lower-bound>* and *<upper-bound>*.
- **AUIF501I**
  NO NEW CATALOGED SMF DATA SETS FOUND FOR SMF MASK: *smf_mask_value*
- **AUIF502I**
  PROCESSING SMF DATA SET: *smf_data_set_name*
- **AUIF503I**
  PROCESSING COMPLETE FOR SMF DATA SET: *smf_data_set_name*
- **AUIF505I**
  SMF AUDITING IS DISABLED AT THE AGENT LEVEL
- **AUIF506I**
  SMF AUDITING IS DISABLED AT THE IMS LEVEL. IMS NAME: *ims_name*
- **AUIF507E**
  PROCESSING FAILED FOR SMF DATA SET: *data set name*
- **AUIF508I**
  SCANNING RECON DATA SETS FOR IMS ARTIFACT DATA SETS. **RECON1:** *recon1_dsn* **RECON2:** *recon2_dsn* **RECON3:** *recon3_dsn*
- **AUIF702I**
  SMF MASK CHECKPOINT INFORMATION - MASK VALUE : *SMF_mask* - LAST DSN READ: *SMF_dsn* - LAST UPDATED (UTC): *date_time*

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIF002I SMF log reader interval set to *<n>* minutes.

Explanation

The subtask that reads event data from SMF log data sets is scheduled to perform every <n> minutes.

User response

No action is required.
Parent topic: Error messages and codes: AUIFxxxx

AUIF003E Command *<command>* failed; interval value must be between *<lower-bound>* and *<upper-bound>*.

Explanation

This message indicates that *<command>* such as:

```
/f AUIASTC,SET INTERVAL <number>
```

failed because of incorrect *<number>* value. Correct value must be between <lower-bound> and <upper-bound>.

User response

Use an interval value between *<lower-bound>* and *<upper-bound>*. If that does not resolve the issue, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIFxxxx

AUIF501I NO NEW CATALOGED SMF DATA SETS FOUND FOR SMF MASK: *smf_mask_value*

Explanation

When scanning the z/OS® catalog for new data sets that meet the indicated SMF mask value (*smf_mask_value*) and have not been processed by the product, it was determined that no z/OS data sets meet that criteria.

System action

The process will continue to examine other SMF Mask values.

User response

No action is required.
Parent topic: Error messages and codes: AUIFxxxx

AUIF502I PROCESSING SMF DATA SET: *smf_data_set_name*

Explanation

Processing has started for a SMF data set.

System action

Events will be obtained from the SMF data set based on collection profile criteria.

User response

None.
Parent topic: Error messages and codes: AUIFxxxx

AUIF503I PROCESSING COMPLETE FOR SMF DATA SET: *smf_data_set_name*

Explanation

Processing of the SMF data set has completed.

System action

Processing continues with other candidate SMF data sets.

User response

No action is required.
Parent topic: Error messages and codes: AUIFxxxx

AUIF505I SMF AUDITING IS DISABLED AT THE AGENT LEVEL

Explanation

Auditing of SMF events has been disabled at the agent level, as instructed by the settings chosen in the Guardium user interface.

System action

The auditing of events sourced from SMF data sets is not performed.

User response

No action is required.
Parent topic: Error messages and codes: AUIFxxxx

AUIF506I SMF AUDITING IS DISABLED AT THE IMS LEVEL. IMS NAME: *ims_name*

Explanation

Auditing of SMF events has been disabled at the IMS level for the IMS named (*ims_name*) by use of the Guardium interface and the IMS Auditing Levels editor.

System action

The auditing of events sourced from SMF for the IMS named is not performed.

User response

If this is a desired action, then no response is needed. If SMF events should be audited for this IMS, then the IMS configuration should be modified by using the Guardium interface and the IMS Auditing Levels to select any or all SMF events you want to audit.
Parent topic: Error messages and codes: AUIFxxxx

AUIF507E PROCESSING FAILED FOR SMF DATA SET: *data set name*

Explanation

Processing failed during the reading of the data set, specified by name in the message text.

System action

The collection process terminates.

User response

Determine the cause of the failure and correct it by reviewing previously issued S-TAP and z/OS messages.
Parent topic: Error messages and codes: AUIFxxxx

AUIF508I SCANNING RECON DATA SETS FOR IMS ARTIFACT DATA SETS. RECON1: *recon1_dsn* RECON2: *recon2_dsn* RECON3: *recon3_dsn*

Explanation

The AUIFSTC task has started to scan the RECON data sets looking for database data sets, Image copy data sets and optionally IMS SLDS to be audited using SMF records.

System action

The RECON data sets are read using the specified DSN.

User response

No action is required.
Parent topic: Error messages and codes: AUIFxxxx

AUIF702I SMF MASK CHECKPOINT INFORMATION - MASK VALUE : *SMF_mask* - LAST DSN READ: *SMF_dsn* - LAST UPDATED (UTC): *date_time*

Explanation

This message provides the SMF data set mask (*SMF_mask*) and the last SMF data set read (*SMF_dsn*) that matched that mask. This information is used as a checkpoint to indicate which SMF data sets have already been processed, and should not be re-read by the AUIFstc tasks.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIFxxxx

Error messages and codes: AUIGxxxx

The following information is about error messages and codes that begin with AUIG.

- **AUIG001S**
  An unexpected error occurred (/path/to/file.c, linenum).
- **AUIG002S**
  An unexpected error occurred with token "token1" (/path/to/file.c,linenum).
- **AUIG003S**
  An unexpected error occurred with tokens "token1" and "token2" (/path/to/file.c,linenum).
- **AUIG004S**
  An unexpected error occurred with tokens "token1", "token2", "token3", and "token4" (/path/to/file.c,linenum).
- **AUIG005S**
  An unexpected error occurred with tokens "token1", "token2", and "token3" (/path/to/file.c,linenum).
- **AUIG006S**
  An unexpected error occurred with tokens "token1" and "token2" (/path/to/file.c,linenum).
- **AUIG014E**
  dataspace create return code = *return-code-hex*, reason = *reason-code-hex*

- **AUIG015W**
  MALLOC: big alloc coming *memory_size* from GDM Read Buffer
- **AUIG016S**
  MALLOC: zero alloc from *<site>*.
- **AUIG017S**
  MALLOC: negative malloc *memory size* at site *site*.
- **AUIG018S**
  MALLOC failed, got NULL for size *<memory_size>* at site *<site>*.
- **AUIG045E**
  Write failed, sd=*bbbb* desired write len *length* buffer at *address*, ret code *xxxx* reason 0x*yyyyzzzz*
- **AUIG046E**
  Failure to resolve address for host *'HOST'*, ret code *return-code*, reason *hex-value*.
- **AUIG047E**
  Set sockopt failed, level = *hex-value*, option = *hex-value*, ret code *return-code*, reason *hex-value*.
- **AUIG048E**
  Get sockopt failed, ret code *return-code*, reason *hex-value*.
- **AUIG049E**
  BPXFCT failed, ret code *<return-code>*; reason *<reason-code>*.
- **AUIG050E**
  Read failed ret code *xxxx* reason 0x*zzzzzzzz*
- **AUIG051I**
  TCP write disabled
- **AUIG052I**
  Write to megabuffer disabled
- **AUIG053I**
  Unexpected payload received *<hexadecimal string>*. Payload ignored.
- **AUIGF120I**
  Trace Settings: Compilation 0, Requested Runtime 0, ECSA Flag 32, Actual Runtime 0...
- **AUIGF201I**
  Valid stage zero filter criteria found.
- **AUIGF202I**
  No valid stage zero filter criteria found.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIG001S An unexpected error occurred (/path/to/file.c, linenum).

Explanation

An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG002S An unexpected error occurred with token "token1" (/path/to/file.c,linenum).

Explanation

An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG003S An unexpected error occurred with tokens "token1" and "token2" (/path/to/file.c,linenum).

Explanation

An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG004S An unexpected error occurred with tokens "token1", "token2", "token3", and "token4" (/path/to/file.c,linenum).

Explanation

An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response

Contact IBM® Software Support
Parent topic: Error messages and codes: AUIGxxxx

AUIG005S An unexpected error occurred with tokens "token1", "token2", and "token3" (/path/to/file.c,linenum).

Explanation

An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG006S An unexpected error occurred with tokens "token1" and "token2" (/path/to/file.c,linenum).

Explanation

An unknown and unexpected internal error occurred in the product due to the specified tokens.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG014E dataspace create return code = *return-code-hex*, reason = *reason-code-hex*

Explanation

An attempt to create a data space for spill usage has failed. Spill capability might not be available.

User response

Examine the return code and reason code, and take appropriate action to ensure that data spaces can be created.
Parent topic: Error messages and codes: AUIGxxxx

AUIG015W MALLOC: big alloc coming *memory_size* from GDM Read Buffer

Explanation

More than 10,485,760 bytes was required in order to process collection policies pushed from the Security Guardium® system.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIGxxxx

AUIG016S MALLOC: zero alloc from *<site>*.

Explanation

Zero bytes was required in order to process collection policies pushed from the Security Guardium® system.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG017S MALLOC: negative malloc *memory size* at site *site*.

Explanation

Negative number of bytes required in order to process collection policies pushed from the Security Guardium® system.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG018S MALLOC failed, got NULL for size *<memory_size>* at site *<site>*.

Explanation

Attempt to allocate memory failed.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG045E Write failed, sd=*bbbb* desired write len *length* buffer at *address*, ret code *xxxx* reason 0x*yyyyzzzz*

Explanation

An attempt to read or write to a socket has failed. This error might occur if Security Guardium® S-TAP® for IMS is connected to a peer that is offline.

System action

The system attempts to reestablish the connection to the peer in order to read or write the data.

User response

Identify the cause of the failure by using the *z/OS® UNIX System Services Messages and Codes SA23-2284-xx* manual to look up the return and return codes that are provided in the message text, where *bbbb* is an internal code, *xxxx* is the return code, and *yyyyzzzz* is the reason code. Use the *zzzz* value to determine the error code, as described in the Reason codes (errnojrs) section of the *z/OS UNIX System Services Messages and Codes* manual.
Parent topic: Error messages and codes: AUIGxxxx

AUIG046E Failure to resolve address for host *'HOST'*, ret code *return-code*, reason *hex-value*.

Explanation

An attempt to resolve the given hostname failed.

User response

Verify that the hostname is specified correctly and is resolvable. Contact IBM® Software Support if hostname is correct and resolvable.
Parent topic: Error messages and codes: AUIGxxxx

AUIG047E Set sockopt failed, level = *hex-value*, option = *hex-value*, ret code *return-code*, reason *hex-value*.

Explanation

An attempt to set a socket option failed.

User response

Contact IBM® Software Support
Parent topic: Error messages and codes: AUIGxxxx

AUIG048E Get sockopt failed, ret code *return-code*, reason *hex-value*.

Explanation

An attempt to set a socket option failed.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIGxxxx

AUIG049E BPXFCT failed, ret code *<return-code>*; reason *<reason-code>*.

Explanation

The system BPXFCT call failed while attempting to set socket blocking mode.

User response

See the *MVS Programming: Authorized Assembler Services Guide* for more information about the specified information and error codes.
Parent topic: Error messages and codes: AUIGxxxx

AUIG050E Read failed ret code *xxxx* reason 0x*zzzzzzzz*

Explanation

An attempt to read or write to a socket has failed. This error might occur if Security Guardium® S-TAP® for IMS is connected to a peer that is offline.

System action

The system attempts to reestablish the connection to the peer in order to read or write the data.

User response

Identify the cause of the failure by using the z/OS USS Return Codes and Reason Codes to look up the return and reason codes that are provided in the message text, where *xxxx* is the return code and *zzzzzzzz* is the reason code.
Parent topic: Error messages and codes: AUIGxxxx

AUIG051I TCP write disabled

Explanation

TCP/IP processing has been disabled.

System action

The Guardium appliance will not receive data.

User response

No action is required.
Parent topic: Error messages and codes: AUIGxxxx

AUIG052I Write to megabuffer disabled

Explanation

TCP/IP buffer has been disabled.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIGxxxx

AUIG053I Unexpected payload received *<hexadecimal string>*. Payload ignored.

Explanation

An unexpected string of data was received by the Security Guardium® S-TAP® for IMS agent from the Guardium appliance or associated firewall. The string does not conform to the format that is normally associated with a pushed-down policy or other expected data.

System action

The string is ignored and normal processing continues.

User response

If this message appears occasionally, no action is required. If this message appears frequently, contact IBM Support to diagnose whether a problem exists with the Guardium appliance or firewall.
Parent topic: Error messages and codes: AUIGxxxx

AUIGF120I Trace Settings: Compilation 0, Requested Runtime 0, ECSA Flag 32, Actual Runtime 0...

Explanation

This message is produced during the compilation of a filter, using the policy information that was specified.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIGxxxx

AUIGF201I Valid stage zero filter criteria found.

Explanation

The collection profile compilation process found that the collection profile criteria will allow for Stage zero filtering of IMS DLI events based on USERIDs or PSB names.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIGxxxx

AUIGF202I No valid stage zero filter criteria found.

Explanation

The collection profile compilation process found that the collection profile criteria is not conducive to providing Stage 0 filtering for IMS DLI events. The reasons may include:

- No USERIDS or PSBS were specified in the selection criteria.
- Multiple RULES were defined and differences in the USERID and/or PSB specifications in each rule were different.

System action

Processing continues without Stage Zero filtering capability.

User response

If Stage 0 filtering is desired, adjust the USERID and PSB specifications in each rule to be the same.
Parent topic: Error messages and codes: AUIGxxxx

Error messages and codes: AUIIxxxx

The following information is about error messages and codes that begin with AUII.

Note: To set a z/OS message alert for messages that begin with AUII, use single-dash formatting between the message number and message text. For example:

```
AUII056I
- ZIIP PROCESSING ENABLED FOR IMS STAP
```

- **AUII017I**
  S-TAP® for V10.1.3 initialization complete using RECON1 DSN: *recon1_dsn*
- **AUII018E**
  IBM® Security Guardium® S-TAP for IMS on z/OS® initialization failed
- **AUII019E**
  IBM Security Guardium S-TAP for IMS on z/OS termination failed
- **AUII020E**
  UNABLE TO FIND RECON1 DATA SET NAME

- **AUII021E**
  BLDL FAILED FOR ACTION MODULE *module_name*
- **AUII022E**
  INSUFFICENT STORAGE AVAILABLE FOR *module_name* ACTION MODULE (*stg_type*)
- **AUII023E**
  IMODULE DIRLOAD FAILED FOR ACTION MODULE *module_name*
- **AUII024E**
  Unable to locate IMS SCD address.
- **AUII025E**
  Unable to locate IMS SSCD Extension address.
- **AUII026E**
  UNABLE TO LOCATE THIS IMS SSCT ADDRESS
- **AUII027E**
  INSUFFICIENT STORAGE AVAILABLE FOR AUIPLOG CONTROL BLOCK
- **AUII028E**
  IMODULE LOAD OF ACTION MODULE *module_name* FAILED
- **AUII029E**
  DFSTCBTB LOCATE SERVICE CALL FAILED
- **AUII031E**
  STAP FOR IMS INTERNAL LOGIC ERROR *(rc)*
- **AUII038E**
  ITASK CREATE FOR ACTION MODULE *module_name* FAILED
- **AUII040E**
  ODBA LOAD OF DFSISSI0 FAILED
- **AUII041E**
  ODBA HOOK POINT NOT FOUND (module_name)
- **AUII042W**
  ZIIP PROCESSOR NOT AVAILABLE ON THIS LPAR
- **AUII043W**
  THIS IMS IS NOT CONNECTED TO WORKLOAD MANAGER
- **AUII044E**
  ZIIP PROCESSING REQUEST HAS BEEN REJECTED
- **AUII046E**
  NAME/TOKEN SERVICE *service-name* SERVICE FAILED (*name value*)
- **AUII049E**
  DEDB CALL ANALYSIS INIT FAILURE RC = *return code*
- **AUII050I**
  S-TAP FOR IMS AUDIT STATISTICS
- **AUII052I**
  `USING IMS STAP V10.1.3 MODULE Module_name APAR# Build_date`
- **AUII055I**
  ZIIP PROCESSING HAS BEEN REQUESTED FOR IMS STAP
- **AUII056I**
  ZIIP PROCESSING ENABLED FOR IMS STAP
- **AUII057I**
  process_type PROCESSING FAILED *RC*: return_code *RSN*: reason_code
- **AUII058A**
  STAP FOR IMS COMPONENT HAS ABENDED
- **AUII060W**
  Potential waited PST=*xxxxxxxx* (PST# = *yyyy*)
- **AUII061I**
  Potential Waited PST xxxxxxxx (PST#= zzzz) RELEASED.
- **AUII120I**
  NO COLLECTIONS ACTIVE FOR THIS IMS INSTANCE
- **AUII172I**
  AUIprogram LOADED EXIT *imsexit* FROM DATA SET: *data set name*
- **AUII173E**
  IMS RELEASE *ims-vrl* IS NOT SUPPORTED
- **AUII174E**
  LOAD OF SERVICE MODULE *module_name* FAILED RC = *return_code*
- **AUII175I**
  NON_ZERO RC FROM EXIT *exit_name*: RC = *return_code*
- **AUII176E**
  module_name service_type SERVICE ERROR: RC: *return_code* RS: *reason_code*
- **AUII177E**
  module_name FOUND WITH RENT/REUS ATTRIBUTE IN NON_APF ENVIRONMENT
- **AUII178E**
  DATA SET NAME: *dsn*

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUII017I S-TAP® for V10.1.3 initialization complete using RECON1 DSN: *recon1_dsn*

Explanation

IBM® Guardium® S-TAP for IMS has initialized in the DLI/DBB batch job or IMS control region environment. For successful auditing to occur, the RECON1 DSN indicated in this message should match the RECON1 DSN associated with the IMS definition you have created.

User response

No action is required.
Parent topic: Error messages and codes: AUIIxxxx

AUII018E IBM® Security Guardium® S-TAP® for IMS on z/OS® initialization failed

Explanation

IBM Guardium S-TAP for IMS was unable to initialize in this IMS Control region. The monitoring of IMS databases will not occur.

System action

IMS processing continues without auditing capabilities.

User response

Examine the JES log for other messages to determine the reason for the initialization failure.
Parent topic: Error messages and codes: AUIIxxxx

AUII019E IBM® Security Guardium® S-TAP® for IMS on z/OS® termination failed

Explanation

IBM Guardium S-TAP for IMS was unable to terminate cleanly.

System action

The termination of the IMS online region of DLI/DBB batch job step continues.

User response

This error indicates that an environmental error has occurred. Examine the JES log for other AUI messages to determine the reason for the termination failure.
Parent topic: Error messages and codes: AUIIxxxx

AUII020E UNABLE TO FIND RECON1 DATA SET NAME

Explanation

An attempt to find the RECON1 data set name used by the IMS Online control region or DLI/DBB batch job step has failed. The RECON1 data set name is critical to the determination of the collection profile used to audit IMS events.

System action

IMS processing continues without the IMS auditing feature.

User response

Determine why the RECON1 data set name is not available for this IMS control region or DLI/DBB batch job step. An in-stream RECON1 DD statement must be present in the JCL, or a RECON1 MDALIB member being present in the JOB/STEPLIB DD concatenation is required.
Parent topic: Error messages and codes: AUIIxxxx

AUII021E BLDL FAILED FOR ACTION MODULE *module_name*

Explanation

An attempt to find a required processing module (module_name) has failed.

System action

IMS processing continues without auditing.

User response

Examine the STEPLIB/JOBLIB DD concatenation to ensure the SAUIIMOD product data set is included.
Parent topic: Error messages and codes: AUIIxxxx

AUII022E INSUFFICENT STORAGE AVAILABLE FOR *module_name* ACTION MODULE (*stg_type*)

Explanation

An attempt to obtain storage for the module named (*module_name*) has failed. The storage type field (*stg_type*) indicates if the storage required is 31bit or 24bit based.

System action

IMS processing continues without IMS auditing available.

User response

Increase the region size used by the job step (REGION=).
Parent topic: Error messages and codes: AUIIxxxx

AUII023E IMODULE DIRLOAD FAILED FOR ACTION MODULE *module_name*

Explanation

The DIRLOAD IMS service has failed.

System action

IMS processing continues with auditing.

User response

Determine the cause of the error from the IMS Messages and Codes manual and correct the error. If necessary, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII024E Unable to locate IMS SCD address.

Explanation

An attempt to locate the IMS SCD during product initialization has failed.

System action

IMS processing continues without auditing.

User response

Verify that you are attempting to run the product using a supported IMS release. Contact IBM® Software Support for further assistance.
Parent topic: Error messages and codes: AUIIxxxx

AUII025E Unable to locate IMS SSCD Extension address.

Explanation

An attempt to locate the IMS SSCD Extension address has failed.

System action

IMS processing continues without auditing.

User response

Verify that you are attempting to run the product using a supported IMS release. Contact IBM Software Support for further assistance.
Parent topic: Error messages and codes: AUIIxxxx

AUII026E UNABLE TO LOCATE THIS IMS SSCT ADDRESS

Explanation

The IMS SCCT address cannot be located by the IMS S-TAP initialization process.

System action

IMS processing continues without auditing capabilities.

User response

Contact IBM Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII027E INSUFFICIENT STORAGE AVAILABLE FOR AUIPLOG CONTROL BLOCK

Explanation

An attempt to obtain E/CSA to hold the AUIPLOG module has failed.

System action

IMS processing continues without auditing.

User response

Investigate E/CSA usage on the LPAR.
Parent topic: Error messages and codes: AUIIxxxx

AUII028E IMODULE LOAD OF ACTION MODULE *module_name* FAILED

Explanation

An attempt to LOAD module module_name using IMS services has failed.

System action

An attempt to LOAD module module_name using IMS services has failed.

User response

Verify that the SAUIIMOD product data set is available in the STEPLIB/JOBLIB data set concatenation. Contact IBM® Software Support for further assistance.
Parent topic: Error messages and codes: AUIIxxxx

AUII029E DFSTCBTB LOCATE SERVICE CALL FAILED

Explanation

A call to the IMS DFSTCBTB service has failed.

System action

IMS processing continues without auditing.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII031E STAP FOR IMS INTERNAL LOGIC ERROR *(rc)*

Explanation

Security Guardium® S-TAP® for IMS initialization found a logic error.

System action

IMS processing continues without auditing.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII038E ITASK CREATE FOR ACTION MODULE *module_name* FAILED

Explanation

DA call to the DFSCIR IMS service to create an ITASK has failed.

System action

IMS processing continues without auditing.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII040E ODBA LOAD OF DFSISSI0 FAILED

Explanation

An attempt to LOAD IMS module DFSISSI0 has failed.

System action

IMS processing with auditing continues. The product will be unable to determine the correct USERID for events driven from ODBA threads.

User response

Contact Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII041E ODBA HOOK POINT NOT FOUND (module_name)

Explanation

An attempt to locate a hook point in the indicated module (module_name) has failed.

System action

IMS processing with auditing continues. The product will be unable to determine the correct USERID for events driven from ODBA threads. An output DD: AUI$NAP is dynamically allocated to SYSOUT, and the area where the hook point was to be located is snapped out to this AUI$NAP DD.

User response

Provide the AUI$NAP output to IBM Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII042W ZIIP PROCESSOR NOT AVAILABLE ON THIS LPAR

Explanation

The AUIZIIP DD statement has been found in the IMS Control Region JCL, which indicates that the zIIP processor should be considered for use when filtering DLI calls and writing to the z/OS® System Logger. IMS STAP has determined that zIIP processing is not available on this LPAR.

System action

Processing continues exclusively using general processors.

User response

Remove the AUIZIIP DD statement and restart the IMS sub-system.
Parent topic: Error messages and codes: AUIIxxxx

AUII043W THIS IMS IS NOT CONNECTED TO WORKLOAD MANAGER

Explanation

A request to process DLI call filtering and z/OS® System Logger writes on a zIIP processor has been rejected as the IMS sub-system is not connected to the z/OS Workload Manager.

System action

Processing continues exclusively using general processors.

User response

No action is required.
Parent topic: Error messages and codes: AUIIxxxx

AUII044E ZIIP PROCESSING REQUEST HAS BEEN REJECTED

Explanation

A request to process DLI call filtering and z/OS® System Logger writes on a zIIP processor has been rejected.

System action

Processing continues exclusively using general processors.

User response

Review previously issued AUII messages to determine the root cause of the request rejection.
Parent topic: Error messages and codes: AUIIxxxx

AUII046E NAME/TOKEN SERVICE *service-name* SERVICE FAILED (*name value*)

Explanation

An attempt to drive the z/OS® name/token service has failed.

System action

IMS processing continues without auditing.

User response

Contact IBM® Software Support
Parent topic: Error messages and codes: AUIIxxxx

AUII049E DEDB CALL ANALYSIS INIT FAILURE RC = *return code*

Explanation

An attempt insert product code in the DEDB call analysis area has failed.

System action

IMS processing with DEDB event auditing disabled. An output DD: AUI$NAP is dynamically allocated to SYSOUT, and the area where the code insertion was to be located is snapped out to this AUI$NAP DD.

User response

Provide the AUI$NAP output to IBM® Software Support.
Parent topic: Error messages and codes: AUIIxxxx

AUII050I S-TAP® FOR IMS AUDIT STATISTICS

Explanation

This message provides statistics regarding the number of DLI events which have been processed. This message is issued when:

- The number of DLI calls specified in the message frequency section of the Guardium client's IMS Data Set definition screen has been reached.
- The time specified in the AUII050I message frequency section of the Guardium client's IMS Data Set definition screen has elapsed.
- The collection profile for the IMS is made in active.
- The DLI/DBB batch job or IMS Online Control Region terminates.

The description of values are as follows:

DLI CALLS RECEIVED
: This value indicates the number of IMS DLI calls which had the potential of being audited. This number can be more or less than the number of actual DLI calls performed, because:

  - DLI PATH calls which effect multiple segments within a hierarchical path are treated and counted as individual DLI calls.
  - DLI calls types which are not included in any RULE of the active collection profile are not counted as they are immediately rejected.

DLI CALLS AUDITED
: This value indicates the number of IMS DLI calls which resulted in a DLI event being written to the z/OS® System Logger Log-stream for transmittal to the Guardium® Appliance.

IXGWRITE ERRORS
: This value indicates the number of z/OS System Logger IXGWRITE calls which have failed. One of more AUIJ304E messages will precede the issuance of the AUII050I message if the number of IXGWRITE errors is greater than zero. A non-zero value for the IXGWRITE ERRORS and a zero value for the DLI CALLS LOST DUE TO IXGWRITE ERRORS section of this message indicates that the IXGWRITE errors were subsequently retried and the IXGWRITE calls were then completed successfully.

DLI CALLS LOST DUE TO IXGWRITE ERRORS
: A non-zero value in this section indicates that DLI calls which were audited and either:

  - Could not be placed into a log-stream data buffer (indicated by the issuance of message AUIJ307A).
  - Audited events already in the data buffer could not be written to the z/OS System Logger Log-Stream using the IXGWRITE call and the collection profile for the IMS has been deactivated or the DLI/DBB batch job or IMS Online Control region has been terminated (indicated by the issuance of message AUIJ304E).

System action

Processing continues.

User response

No action is required. This is an informational message only.
Parent topic: Error messages and codes: AUIIxxxx

AUII052I USING IMS STAP V10.1.3 MODULE *Module_name APAR# Build_date*

Explanation

These messages are issued by the IMS S-TAP® code in the IMS Control region during startup to broadcast the maintenance level of the programs that are in use by Security Guardium® S-TAP for IMS.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIIxxxx

AUII055I ZIIP PROCESSING HAS BEEN REQUESTED FOR IMS STAP

Explanation

The AUIZIIP DD statement has been found in the IMS Control Region JCL, which indicates that the zIIP processor should be considered for use when filtering DLI calls and writing to the z/OS® System Logger.

System action

IMS STAP attempts to create an environment to support zIIP processing.

User response

If this was not intended, remove the AUIZIIP DD statement and restart the IMS sub-system.
Parent topic: Error messages and codes: AUIIxxxx

AUII056I ZIIP PROCESSING ENABLED FOR IMS STAP

Explanation

The request for zIIP support for IMS STAP and this IMS Control Region has been acted on and all initialization processes have completed successfully.

System action

IMS STAP will schedule DLI call filtering and writes to the z/OS® System Logger as a zIIP eligible enclave SRB.

User response

If this was not intended, remove the AUIZIIP DD statement and restart the IMS sub-system.
Parent topic: Error messages and codes: AUIIxxxx

AUII057I *process_type* PROCESSING FAILED *RC*: return_code *RSN*: reason_code

Explanation

The AUIZIIP DD statement has been found in the IMS Control Region JCL, which indicates that the zIIP processor should be considered for use when filtering DLI calls and writing to the z/OS® System Logger. A process (process_type) used to enable zIIP processing has failed.

System action

The request to enable zIIP processing is rejected and general processor will be used.

User response

Review IBM® supplied documentation for the process which failed using the return and reason codes (*return_code/reason_code*) to determine the cause of the failure.
Parent topic: Error messages and codes: AUIIxxxx

AUII058A STAP FOR IMS COMPONENT HAS ABENDED

Explanation

The S-TAP® for IMS component has abnormally ended, causing auditing to disable.

User response

Contact IBM® Software Support
Parent topic: Error messages and codes: AUIIxxxx

AUII060W Potential waited PST=*xxxxxxxx* (PST# = *yyyy*)

Explanation

This warning message indicates that IBM® Guardium® S-TAP® for IMS has detected a dependent region that has been waiting for an event to be audited for at least 15 seconds. The dependent region is identified by the PST address *xxxxxxxx*. The PST# value specified as *yyyy* is the region number in hexadecimal format.

System action

IBM Guardium S-TAP for IMS attempts to process the dependent region.

User response

If the dependent region continues processing, then no action is required. If the dependent region remains in a wait state, then it must be stopped or cancelled. Before you stop or cancel the dependent region, take an SVC dump of the IMS Control region and provide it to IBM Software Support for analysis.
Parent topic: Error messages and codes: AUIIxxxx

AUII061I Potential Waited PST xxxxxxxx (PST#= zzzz) RELEASED.

Explanation

This message is a response to message AUII060W (Potential Waited PST xxxxxxxx (PST#= zzzz)). This message indicates that the corresponding IPOST was performed, and the PST is no longer in a WAIT state.

System action

IMS Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIIxxxx

AUII120I NO COLLECTIONS ACTIVE FOR THIS IMS INSTANCE

Explanation

Initialization has completed successfully for Security Guardium® S-TAP® for IMS, but no collections were found that pertain to this batch job or IMS control region.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIIxxxx

AUII172I *AUIprogram* LOADED EXIT *imsexit* FROM DATA SET: *data set name*

Explanation

The *AUIprogram* named found an occurrence of the *imsexit* later within the JOBLIB/STEPLIB concatenation, and has loaded it.

System action

The *imsexit* will be invoked with R13 pointing to the save area originally provided by IMS, as well as its own 512 byte work area, provided in the SXPLAWRK field of the IMS Standard User Exit Parameter list, immediately following each execution of *AUIprogram*.

User response

For the *imsexit* to run, no action is required. If the *imsexit* should not be run in this environment, remove the data set from the JOBLIB/STEPLIB concatenation and restart the IMS control region or batch job.
Parent topic: Error messages and codes: AUIIxxxx

AUII173E IMS RELEASE *ims-vrl* IS NOT SUPPORTED

Explanation

The IMS release being used is not support by this version of the product.

System action

IMS processing continues without auditing.

User response

Review supported IMS releases for the release of this product.
Parent topic: Error messages and codes: AUIIxxxx

AUII174E LOAD OF SERVICE MODULE *module_name* FAILED RC = *return_code*

Explanation

LOAD OF SERVICE MODULE *module_name* FAILED RC = *return_code*

User response

Ensure that the SAUIIMOD product data set is included in the STEPLIB/JOBLIB DD concatenation.
Parent topic: Error messages and codes: AUIIxxxx

AUII175I NON_ZERO RC FROM EXIT *exit_name*: RC = *return_code*

Explanation

The *exit_name* indicated returned a non-zero return code value of *return_code* as specified.

System action

The return code value is returned to IMS.

User response

Correct the *exit_name* program if the non-zero value was returned in error. Review the IMS Customization Guide or IMS Exit Routine Reference for more information.
Parent topic: Error messages and codes: AUIIxxxx

AUII176E *module_name service_type* SERVICE ERROR: RC: *return_code* RS: *reason_code*

Explanation

The *service_type* invoked by the specified *module_name* has failed.

System action

IMS processing continues without auditing.

User response

Review all subsequent AUI error messages to diagnose the problem.
Parent topic: Error messages and codes: AUIIxxxx

AUII177E *module_name* FOUND WITH RENT/REUS ATTRIBUTE IN NON_APF ENVIRONMENT

Explanation

Program *module_name* had the RENT/REUS attribute on in a non-APF-Authorized environment. Security Guardium® S-TAP® for IMS is unable to load the program.

System action

Processing continues with the exit cascading feature disabled.

User response

Re-link the exit with the NOREUSE attribute.
Parent topic: Error messages and codes: AUIIxxxx

AUII178E DATA SET NAME: *dsn*

Explanation

This message is issued in conjunction with a previous message (for example, AUII176E) to indicate an associated data set.

User response

Check the log for the previously issued, associated message and take the action that is advised in that message.
Parent topic: Error messages and codes: AUIIxxxx

Error messages and codes: AUIJxxxx

The following information is about error messages and codes that begin with AUIJ.

- **AUIJ005W**
  UNABLE TO LOAD MESSAGE TABLE *table_name* RSN: *reason_code* WILL USE AUIMGENU
- **AUIJ006E**
  LOAD FAILED FOR MESSAGE TABLE *table_name* RSN: *reason_code*
- **AUIJ007E**
  PROGRAM *program_name* IS NOT EXECUTING APF-AUTHORIZED
- **AUIJ008I**
  ATTEMPTING TO CONNECT TO THE GUARDIUM S-TAP® APPLIANCE. **TCP/IP Address:** *ip_address*, **PORT:** *port_number*, **PING RATE:** *ping_rate*
- **AUIJ009E**
  LOAD FAILED FOR MODULE *module_name*. R1: *abend_code* R15: *reason_code*
- **AUIJ010I**
  IMS STAP *ver* HAS STARTED.
- **AUIJ011I**
  function_type CALL TO GUARDUIM S-TAP APPLIANCE SUCCESSFUL
- **AUIJ012I**
  NUMBER OF *event_type* EVENTS SENT TO APPLIANCE: *counter*
- **AUIJ013E**
  stap_call TO GUARDUIM S-TAP APPLIANCE FAILED *(call source)* IP ADDRESS: *ip_address* STAP_RC = *rc1* STAP_RS = *rs1* GDM_RC = *rc2* PB_RC = *rc3* GDML_RC = *rc4* GDML_RS = *rs2*
- **AUIJ014E**
  OPEN FAILED FOR DD *dd_name*
- **AUIJ015E**
  THIS IMS RELEASE IS NOT SUPPORTED. IMS NAME: *ims-name*, VRL: *ims_version*
- **AUIJ016E**
  UNABLE TO INITIALIZE APPLIANCE INTERFACE *(connection_type)*
- **AUIJ017I**
  PRIMARY STAP CONNECTION RESTORED *(connection_type)* - SUCCESSFULLY CONNECTED TO IP ADDRESS: *ip_address* - PORT : *port*
- **AUIJ018W**
  PREVIOUS STAP CONNECTION FAILED *(connection_type)* - SUCCESSFULLY CONNECTED TO IP ADDRESS: *ip_address* - PORT : *port*
- **AUIJ019E**
  STAP CONNECTION FAILED: NO CONNECTIONS AVAILABLE *(connection_type)* - IP ADDRESS: *ip-address* - PORT : *port*
- **AUIJ020I**
  All EVENTS HAVE BEEN WRITTEN FROM SPILL AREA TO APPLIANCE *(connection_type)*
- **AUIJ021W**
  EVENTS ARE BEING WRITTEN TO THE SPILL AREA *(connection_type)*
- **AUIJ022W**
  SPILL AREA IS FULL: EVENT DATA IS BEING LOST *(connection_type)*
- **AUIJ023E**
  SPILL AREA IS NOT AVAILABLE *(connection_type)*
- **AUIJ024W**
  NUMBER OF *type* EVENTS LOST *count*
- **AUIJ042W**
  ZIIP PROCESSING NOT AVAILABLE ON THIS LPAR (type)
- **AUIJ044W**
  ZIIP PROCESSING REQUEST HAS BEEN REJECTED *(connection_type)*
- **AUIJ055I**
  ZIIP PROCESSING REQUESTED FOR *type* PROCESSING
- **AUIJ056I**
  ZIIP PROCESSING ENABLED FOR type PROCESSING, ENCLAVE TOKEN: *value*
- **AUIJ057W**
  ZIIP PROCESSING FOR *type* EVENTS HAS BEEN DISABLED DUE TO ERRORS - PROCESSING WILL CONTINUE USING GCPU
- **AUIJ058W**
  ZIIP PROCESSING FOR *type* EVENTS HAS BEEN DISABLED - TRACING IS ENABLED BY THE USE OF THE AUI$NAP JCL STATEMENT
- **AUIJ201E**
  VSAM ERROR ENCOUNTERED
- **AUIJ202E**
  VSAM ERROR ENCOUNTERED
- **AUIJ203E**
  VSAM ERROR ENCOUNTERED
- **AUIJ250I**
  AUDITING IMS EVENTS. COLLECTION PROFILE NAME: *collection_profile_name* IMS NAME: *ims_name* AGENT NAME: *agent name* EXCLUDED REGIONS: *region_types*

- **AUIJ251E**
  COMPILED FILTER BUILD FAILED. COLLECTION PROFILE NAME : *collection _profile_name* RC: *return_code* RSN: *reason_code*
- **AUIJ252W**
  GUARDIUM QUARANTINE IS IN EFFECT; DBPCB STATUS CODES OF *AI* MAY OCCUR
- **AUIJ255I**
  AUII050I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID: *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*
- **AUIJ256I**
  AUIJ250I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID : *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*
- **AUIJ257I**
  AUII120I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID: *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*
- **AUIJ258I**
  AUII052I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID: *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*
- **AUIJ259I**
  JOBNAME *job_name* USING IMS STAP V10.1.3 MODULE: *pgm_name* APAR: *fix_number* DATE: *fix_date*
- **AUIJ303W**
  request_type REQUEST FOR LOG STREAM *log_stream_name* FAILED - RC: *return_code* RS: *reason_code* - WILL CONTINUE TO RETRY
- **AUIJ304A**
  IXGCONN REQUEST FOR LOG_STREAM *log_stream_name* FAILED with RC = *return_code* and RS= *reason_code*
- **AUIJ304E**
  IXGWRITE REQUEST FOR *<log-stream-name>* FAILED - RC: *return_code* RS: *reason_code*
- **AUIJ307A**
  AUDITED EVENTS ARE BEING LOST DUE TO IXGWRITE ERRORS AND/OR BUFFER SHORTAGES
- **AUIJ307E**
  thread_type THREAD IS TERMINATING DUE TO PROCESSING ERRORS.
- **AUIJ330E**
  REQUIRED DATA SET IS NOT CATALOGED. - TYPE: *dsn_type*, DSN: *data_set_name*
- **AUIJ331E**
  service_name SERVICE FAILED - RC: *return_code* - RSN: *reason_code*
- **AUIJ332E**
  DATA SET IS NOT VALID WITHIN CONTEXT USED - TYPE: *data_set_type,* DSN: *data_set_name*, REASON: *reason*
- **AUIJ333E**
  Service *SERVICE FAILED* for *DATA SET*: *dsn - R15: return_code*
- **AUIJ335W**
  dd_name DD IS PRESENT IN THIS JCL, *dsn_types* WILL NOT BE AUDITED
- **AUIJ400E**
  INSUFFICIENT MEMORY - MODULE NAME: *program_name* - MEMORY SEGMENT TYPE: *seg_type*
- **AUIJ401E**
  MODULE *module_name* FAILED DURING ATTACH of *program_name* - RETURN CODE: *return_code*
- **AUIJ402E**
  CATALOG SERVICE REQUEST FAILED - MODULE NAME: *module_name* - RC: *return_code* RSN: *reason_code*
- **AUIJ403E**
  DYNAMIC ALLOCATION FAILURE - FUNCTION : *function_code* - DSN: *data-set-name* - RC: *return_code* RSN: *reason_code*
- **AUIJ404E**
  DYNAMIC ALLOCATION FAILURE - FUNCTION: *function_code* -DDN: *dd_name* - RC: *return_code* RSN: *reason_code*
- **AUIJ406W**
  TOO MANY RULES SPECIFIED IN POLICY, REQUEST HAS BEEN TRUNCATED. POLICY: *policy_name*. RULE LIMIT: *max_number_of rules_allowed*
- **AUIJ407I**
  number DATA SETS ADDED TO POLICY *policy_name* FILTER
- **AUIJ408E**
  POLICY *name* RESULTED IN OVER 102400 DATA SETS TO BE AUDITED; DATA SET RESULT SET HAS BEEN TRUNCATED
- **AUIJ500I**
  STARTING *cycle_type* CYCLE
- **AUIJ501I**
  NO NEW CATALOGED SMF DATA SETS FOUND FOR SMF MASK: - *smf_mask_value*
- **AUIJ504I**
  cycle_type CYCLE COMPLETE
- **AUIJ521W**
  CONTROL BLOCK AUIDCCOM NOT FOUND
- **AUIJ510I**
  `ALTERNATE RECON DATA SETS FOUND FOR IMSNAME imsname: RECON1: alt_dsn_1; RECON2: alt_dsn_2, RECON3: alt_dsn_3`
- **AUIJ511E**
  `ALTERNATE RECON DATA SET NOT CATALOGED; DSN:  alt_dsn`
- **AUIJ512E**
  `ALTERNATE RECON DATA SET NOT A VSAM FILE; DSN:  alt_dsn`
- **AUIJ513E**
  `NO VALID ALTERNATE RECON DATA SETS FOUND FOR IMS imsname;  PROCESSING TERMINATED`
- **AUIJ522E**
  INSUFFICIENT E/CSA STORAGE AVAILABLE FOR *control_block* CONTROL BLOCK
- **AUIJ609I**
  event_types ARE BEING EXCLUDED (*excluded_by*)
- **AUIJ800E**
  REQUIRED DD STATEMENT IS MISSING: *dd-name*
- **AUIJ860E**
  VSAM FILE DEFINITION ERROR - DDN: *dd_name* - REASON: *definition_error*
- **AUIJ999E**
  AN INTERNAL LOGIC ERROR HAS OCCURRED - MODULE: module_name RSN: reason_code

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIJ005W UNABLE TO LOAD MESSAGE TABLE *table_name* RSN: *reason_code* WILL USE AUIMGENU

Explanation

An attempt to perform a z/OS® LOAD of the message table named (*table_name*) failed. The reason for the failure is described in the reason code field (*reason_code*). The default U.S. English message table will be used. This message follows the AUI006E message.

System action

Processing continues while using the U.S. English message table.

User response

Determine and correct the cause of the message table load failure.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ006E LOAD FAILED FOR MESSAGE TABLE *table_name* RSN: *reason_code*

Explanation

A z/OS® LOAD attempt failed for the message table (*table_name*) indicated.

System action

If the table name is the U.S. English message table, (AUIMGENU) processing will terminate. Other table names will cause the product to attempt to use the U.S. English message table after issuing the AUIJ005W message continue processing.

User response

Determine and correct the cause of the message table load failure.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ007E PROGRAM *program_name* IS NOT EXECUTING APF-AUTHORIZED

Explanation

The program specified requires APF-Authorization to perform its function.

System action

The program terminates.

User response

Ensure that all data sets included within the STEPLIB DD concatenation of the JCL where this message appeared are APF authorized.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ008I ATTEMPTING TO CONNECT TO THE GUARDIUM S-TAP® APPLIANCE. TCP/IP Address: *ip_address*, PORT: *port_number*, PING RATE: *ping_rate*

Explanation

An attempt is being made to establish a connection with the Guardium® S-TAP appliance using the named TCP/IP address (*ip_address*) and PORT number (*port_number*).

PING RATE (*ping_rate*) indicates how often a message is sent to the appliance to provide the appliance with confirmation that the connection is active. The PINGS are sent at the rate indicated (*ping_rate*) which is shown in hour, minutes, and second (*hh:mm:ss*) format.

System action

The connection to the Guardium S-TAP appliance is attempted.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ009E LOAD FAILED FOR MODULE *module_name*. R1: *abend_code* R15: *reason_code*

Explanation

An attempt to perform a z/OS® LOAD of the named module (module_name) has failed

System action

The function terminates.

User response

Ensure that all required product data sets are included in the STEPLIB DD concatenation of the JCL where this message appeared. The value in R1 (*abend-code*) indicates the ABEND code that would have occurred if the failure had not been trapped by the product. The value in R15 (*reason_code*) indicates the reason code associated with the abend. Documentation regarding the abend codes and possible resolutions can be found in the *IBM® z/OS MVS™ System Code* manual or equivalent.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ010I IMS STAP *ver* HAS STARTED.

Explanation

The Security Guardium® S-TAP® for IMS agent component, using the specified base code level, has started.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ011I *function_type* CALL TO GUARDUIM S-TAP APPLIANCE SUCCESSFUL

Explanation

The function request (*function_type*) to the Guardium® S-TAP® appliance completed successfully. This message usually follows the AUIJ008I message indicating that the connection request has been initiated.

Function request values which can be displayed are:

INIT-DLIB
: Connection request from the tasks which transmits DLI/DBB batch events.

INIT-DLIO
: Connection request from the task which transmits IMS Online DLI events.

INIT_LOG
: Connection request from the task which transmits IMS Archive log events.

INIT-SMF
: Connection request from the task which transmits SMF events.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ012I NUMBER OF *event_type* EVENTS SENT TO APPLIANCE: *counter*

Explanation

By default, this message is issued every 100,000 events sent to the appliance or approximately every 18 minutes. You can modify this frequency by using the agent parameter keyword DLIFREQ. This message provides a status of data being collected and sent to the Guardium® S-TAP® appliance. The count provided (*counter*) is the number of events since the last message was issued. The type of events (*event_type*) can include DLIB (events captured from IMS DLI/DBB batch jobs), DLIO (events captured from IMS Online regions) SMF (events captured from SMF auditing), IMSL (events captured from IMS archive log processing), and MLOG (missing IMS logs found during IMS Archive log processing).

System action

Processing continues.

User response

None action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ013E *stap_call* TO GUARDUIM S-TAP® APPLIANCE FAILED *(call source)* IP ADDRESS: *ip_address* STAP_RC = *rc1* STAP_RS = *rs1* GDM_RC = *rc2* PB_RC = *rc3* GDML_RC = *rc4* GDML_RS = *rs2*

Explanation

The requested call *(call_type)* to the Guardium® S-TAP appliance has failed. A non-zero value GDM_RC field indicates an error.

System action

The process terminates.

User response

Determine the cause of the failure by checking the return and reason code.

- If GDM_RC is not zero, one or more of the PB_RC, GDML_RC and GDML_RS will be set.
- If STAP_RC and STAP_RS are zero but GCM_RC or PB_RC is not zero, an internal error is indicated. Contact IBM® Software Support.
- If STAP_RC and STAP_RS are not zero, contact IBM Software Support.

Parent topic: Error messages and codes: AUIJxxxx

AUIJ014E OPEN FAILED FOR DD *dd_name*

Explanation

A z/OS® OPEN of the data set(s) referenced by the DD named (*dd_name*) failed.

System action

Processing terminates.

User response

Examine the JES log for z/OS issued IEA messages issued regarding this DD statement and take appropriate action.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ015E THIS IMS RELEASE IS NOT SUPPORTED. IMS NAME: *ims-name*, VRL: *ims_version*

Explanation

The IMS named (*ims-name*) was found to be of a release which is not supported by this version of the product.

System action

Processing terminates.

User response

Review the software requirements documented in this user's guide for a list of IMS releases that are supported by this version of the product.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ016E UNABLE TO INITIALIZE APPLIANCE INTERFACE *(connection_type)*

Explanation

An attempt to establish a connection with the appliance has failed.

System action

Processing terminates.

User response

This error is usually due to the TCP/IP address specified in the <appliance-server> parameter of the AUICONFG or other member used in the AUICONFG DD statement used to provide the agent with configuration information being incorrect. This error can also occur if the target of the TCP/IP address is unresponsive.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ017I PRIMARY STAP CONNECTION RESTORED *(connection_type)* - SUCCESSFULLY CONNECTED TO IP ADDRESS: *ip_address* - PORT : *port*

Explanation

Multiple appliances are defined to IBM® Guardium® S-TAP® for IMS, and the primary appliance (ip_address + port) was unavailable for some period of time. This message indicates that the primary appliance has become available and is now being used.

System action

Processing continues sending data to the primary appliance.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ018W PREVIOUS STAP CONNECTION FAILED *(connection_type)* - SUCCESSFULLY CONNECTED TO IP ADDRESS: *ip_address* - PORT : *port*

Explanation

Multiple appliances are defined to the IMS STAP the connection to the active appliance has failed. This message indicates that another secondary appliance (ip_address + port) is now active.

System action

Processing continues sending data to the secondary appliance.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ019E STAP CONNECTION FAILED: NO CONNECTIONS AVAILABLE *(connection_type)* - IP ADDRESS: *ip-address* - PORT : *port*

Explanation

The connection to the active appliance (ip_address + port) has failed and there are no secondary appliances available for use.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ020I All EVENTS HAVE BEEN WRITTEN FROM SPILL AREA TO APPLIANCE *(connection_type)*

Explanation

All audited events that were buffered to the spill area have been sent to the appliance.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ021W EVENTS ARE BEING WRITTEN TO THE SPILL AREA *(connection_type)*

Explanation

A connection to the appliance has been interrupted, and the spill area is being used to buffer audited events until the appliance connection can be reestablished

System action

Processing continues. Audited events are buffered in the spill area.

User response

Investigate the cause of the appliance connection interruption and correct.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ022W SPILL AREA IS FULL: EVENT DATA IS BEING LOST *(connection_type)*

Explanation

A connection to the appliance was interrupted. The spill area was being used to buffer audited events until the appliance connection can be reestablished. The number of audited events that were generated exceeded the number that could be held in the spill area.

System action

Processing continues. Audited events are discarded.

User response

Investigate the cause of the appliance connection interruption and correct. Look for message AUIJ024W, which is issued at task termination or when a connection is reestablished, for the number of lost events.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ023E SPILL AREA IS NOT AVAILABLE *(connection_type)*

Explanation

An attempt to use the spill area to buffer audited events is unsuccessful.

System action

Processing continues. Audited events are discarded.

User response

Specify a value of 1 through 1024 in the SAUISAMP AUICONFG member <SPILL-SIZE> parameter. Review any z/OS error or warning messages that might indicate why the spill area allocation failed.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ024W NUMBER OF *type* EVENTS LOST *count*

Explanation

Attempts to buffer audited events in the spill area have failed. This message indicates the type of audited events (DLIO, DLIB, SMF etc) which were lost (*type*), and the number that were lost (*count*).

System action

Processing continues. Audited events are discarded.

User response

Investigate the cause of the appliance connection interruption and correct.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ042W ZIIP PROCESSING NOT AVAILABLE ON THIS LPAR (type)

Explanation

A request to process data, using a zIIP enabled enclave, has failed because the Workload Manager feature is not available.

System action

Processing continues, using GCPU (General Central Processor Unit) services.

User response

Remove the ZIIP_AGENT_DLI(Y) keyword from the configuration file that is in use, or change the parameter from Y to N.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ044W ZIIP PROCESSING REQUEST HAS BEEN REJECTED *(connection_type)*

Explanation

An attempt to create a zIIP enabled enclave has failed.

System action

Processing continues using GCPU services.

User response

Determine the cause of the failure by reviewing previously issued AUIJ0331E messages and take corrective action.

Parent topic: Error messages and codes: AUIJxxxx

AUIJ055I ZIIP PROCESSING REQUESTED FOR *type* PROCESSING

Explanation

The use of a zIIP enabled enclave has been requested by the use of the ZIIP_AGENT_DLI(Y) configuration file keyword.

System action

An attempt is made to create the enclave.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ056I ZIIP PROCESSING ENABLED FOR type PROCESSING, ENCLAVE TOKEN: *value*

Explanation

A zIIP enabled enclave has been requested and successfully created.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ057W ZIIP PROCESSING FOR *type* EVENTS HAS BEEN DISABLED DUE TO ERRORS - PROCESSING WILL CONTINUE USING GCPU

Explanation

zIIP processing was requested, however due to previously reported errors, this mode of processing could not be enabled.

System action

Processing continues using General Central Processing Unit (GCPU) resources only.

User response

Review the processing log looking for error and warning messages that were issued prior to this message to help determine why zIIP processing could not be initiated.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ058W ZIIP PROCESSING FOR *type* EVENTS HAS BEEN DISABLED - TRACING IS ENABLED BY THE USE OF THE AUI$NAP JCL STATEMENT

Explanation

Event tracing has been enabled through the addition of the AUI$NAP DD SYSOUT=* JCL statement in the agent JCL. The use of zIIP processing has been disabled because event tracing cannot coexist with the zIIP environment.

System action

All processing continues with event tracing on. Processing occurs on the General Central Processing Unit (GCPU).

User response

If the addition of the AUI$NAP DD statement was not intentional, remove it from the agent JCL.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ201E VSAM ERROR ENCOUNTERED

Explanation

FUNCTION

vsam_function
RPL/RECORD TYPE
rpl/record_value
R15
return_code
R0
reason_code
CSI-CALL
function_call
SUBRTN
pgm_routine

While accessing the VSAM repository, an internal logic error was encountered.

System action

Processing terminates.

User response

There are no user actions available for this failure. Contact IBM® Software Support with the content of this message.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ202E VSAM ERROR ENCOUNTERED

Explanation

While accessing the VSAM repository, an internal logic error was encountered.

FUNCTION:
vsam_function
R15:
return_code
ACBOFLGS:
acboflag_value
CSI-CALL:
function_call
SUBRTN:
pgm_routine

System action

Processing terminates.

User response

There are no user actions available for this failure. Contact IBM® Software Support with the content of this message.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ203E VSAM ERROR ENCOUNTERED

Explanation

While accessing the VSAM repository, an internal logic error was encountered.

FUNCTION:
vsam_function
RPL/RECORD TYPE
rpl/record_value
FDBWD:
rpl_fdbwd
OPTCD:
rpl_optcd
CSI-CALL:
function_call
SUBRTN:
pgm_routine

System action

Processing terminates.

User response

There are no user actions available for this failure. Contact IBM Software Support with the content of this message.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ250I AUDITING IMS EVENTS. COLLECTION PROFILE NAME: *collection_profile_name* IMS NAME: *ims_name* AGENT NAME: *agent name* EXCLUDED REGIONS: *region_types*

Explanation

The auditing of IMS events proceeds by using the collection profile (*collection_profile_name*) that is associated with the IMS definition (*ims_name*). The agent name indicates which agent is processing the audited data. Various region types might have been excluded from auditing, such as AER, BMP, CICS, DBCTL, IFP, MPP, ODBA, or NONE.

System action

Auditing continues.

User response

No action is required.
Note: To set a z/OS message alert for this message, use single-dash formatting between the message number and message text; for example, AUIJ250I - AUDITING IMS EVENTS.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ251E COMPILED FILTER BUILD FAILED. COLLECTION PROFILE NAME : *collection_profile_name* RC: *return_code* RSN: *reason_code*

Explanation

An attempt at building a compiled filter using the collection profile named (*collection_profile_name*) failed.

System action

Processing terminates, auditing will not be performed.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ252W GUARDIUM QUARANTINE IS IN EFFECT; DBPCB STATUS CODES OF *AI* MAY OCCUR

Explanation

The Guardium appliance has detected a list of users for whom access is to be restricted for a period of time. This list is based on policy rules and criteria that are set by the Guardium administrator who maintains the auditing rules in your environment.

System action

Processing continues. If a user in the list of quarantined user IDs attempts to issue DB/DLI calls, the DLI call fails. A DB PCB status code of AI, or an AIB return/reason code of 110/C, is returned to the application program.

User response

If access to IMS databases terminate with a DB PCB status code of AI, or an AIB return/reason code of 110/C, contact the Guardium administrator who maintains the auditing rules in your environment to obtain the reason for the quarantine.
Note: To set a z/OS message alert for this message, use single-dash formatting between the message number and message text; for example, AUIJ252W - GUARDIUM QUARANTINE IS IN EFFECT
Parent topic: Error messages and codes: AUIJxxxx

AUIJ255I AUII050I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID: *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*

Explanation

This message echoes message AUII050I, which is generated by the S-TAP code, and can appear in the IMS control region and the DLI/DBB batch job output. This message only appears in the agent if the DISPLAY_IMSMSG_DLIx(Y) configuration option is coded in the AUICONFG file.

System action

Processing continues.

User response

No action is required. See the explanation for message AUII050I for details regarding the available output fields.

Parent topic: Error messages and codes: AUIJxxxx

AUIJ256I AUIJ250I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID : *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*

Explanation

This message echoes message AUIJ250I, which is generated by the S-TAP code, and can appear in the IMS control region and the DLI/DBB batch job output. This message only appears in the agent if the DISPLAY_IMSMSG_DLIx(Y) configuration option is coded in the AUICONFG file.

System action

Processing continues.

User response

No action is required. See the explanation for message AUIJ250I for details regarding the available output fields.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ257I AUII120I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID: *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*

Explanation

This message echoes message AUII120I, which is generated by the S-TAP code, and can appear in the IMS control region and the DLI/DBB batch job output. This message only appears in the agent if the DISPLAY_IMSMSG_DLIx(Y) configuration option is coded in the AUICONFG file.

System action

Processing continues.

User response

No action is required. See the explanation for message AUII120I for details regarding the available output fields.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ258I AUII052I MESSAGE RECEIVED FROM: JOBNAME: *ims_job_name*; SSID: *ims_ssid*; JOB NUMBER: *job_number*; LPAR: *lpar_name*

Explanation

This message echoes message AUII052I, which is generated by the S-TAP code, and can appear in the IMS control region and the DLI/DBB batch job output. This message only appears in the agent if the DISPLAY_IMSMSG_DLIx(Y) configuration option is coded in the AUICONFG file.

System action

Processing continues.

User response

No action is required. See the explanation for message AUII052I for details regarding the available output fields.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ259I JOBNAME *job_name* USING IMS STAP V10.1.3 MODULE: *pgm_name* APAR: *fix_number* DATE: *fix_date*

Explanation

This message echoes message AUII052I, which is generated by the S-TAP code, and can appear in the IMS control region. This message appears in the agent if the DISPLAY_IMSMSG_DLIx(Y) configuration option is coded in the AUICONFG file.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ303W *request_type* REQUEST FOR LOG STREAM *log_stream_name* FAILED - RC: *return_code* RS: *reason_code* - WILL CONTINUE TO RETRY

Explanation

A request (*request_type*) made to the indicated log stream (*log_stream_name*) has failed. This is a recoverable situation and the request will be retried.

System action

Processing will continue with the request being retried.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ304A IXGCONN REQUEST FOR LOG_STREAM *log_stream_name* FAILED with RC = *return_code* and RS= *reason_code*

Explanation

An attempt to connect to the z/OS System Logger log-stream, by using the IXGCONN function, has failed.

System action

Auditing is disabled, but IMS continues processing.

User response

Correct the issue that has caused the IXGCONN failure; then, uninstall and reinstall the policy to cause IMS to reattempt the connection. Or, correct the issue; then, stop and restart the Security Guardium® S-TAP® for IMS agent to cause IMS to reattempt the IXGCONN call.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ304E IXGWRITE REQUEST FOR *<log-stream-name>* FAILED - RC: *return_code* RS: *reason_code*

Explanation

An attempt to write to the z/OS® System Logger log-stream using the IXGWRITE function has failed.

System action

One occurrence of this message is issued once per error type (RC + RSN) within the each issuance of message AUII050I. IXGWRITE calls continues until the collection policy for the IMS system is uninstalled, or the DLI/DBB batch job or IMS control region terminates.

User response

Examine the description of the IXGWRITE error using the RC and RSN codes provided in the IBM® z/OS MVS™ Programming: Assembler Services Reference, Vol. 2 (IAR-XCT) or equivalent, under the IXGWRITE Macro description, and take corrective action. The most common reason for the appearance of this message is the volume and the rate (number of events per second) of DLI events exceeds the capacity of the current z/OS System Logger log stream definition.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ307A AUDITED EVENTS ARE BEING LOST DUE TO IXGWRITE ERRORS AND/OR BUFFER SHORTAGES

Explanation

A number of attempts to write audited events to the z/OS® System Logger Log-stream have failed which has caused has resulted in available space in the data buffers being exhausted. This has resulted in DLI events which are to be audited to be discarded.

System action

DLI events continue to be audited at attempts to write exiting data buffers to the z/OS System Logger Log-stream until. The number of DLI events which were rejected are noted in subsequent AUII050I message.

User response

Review any AUIJ304E messages which have been issued to determine the cause of the z/OS System Logger Log-stream Write failures.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ307E *thread_type* THREAD IS TERMINATING DUE TO PROCESSING ERRORS.

Explanation

The agent has determined that a fatal error or abend occurred in the thread type indicated.

System action

Processing that is associated with this thread will not occur.

User response

Examine previously issued error or abend messages to determine the corrective action to be taken. Then, restart the agent.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ330E REQUIRED DATA SET IS NOT CATALOGED. - TYPE: *dsn_type*, DSN: *data_set_name*

Explanation

The data set name indicated (data_set_name) was not found in the z/OS® catalog.

System action

Processing terminates

User response

Specify the name of a cataloged data set.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ331E *service_name* SERVICE FAILED - RC: *return_code* - RSN: *reason_code*

Explanation

A z/OS® service (*service_name*) failed when executed.

System action

Processing terminates.

User response

Determine the cause of the failure by using the return and reason codes provided. Contact IBM® Software Support for additional assistance.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ332E DATA SET IS NOT VALID WITHIN CONTEXT USED - TYPE: *data_set_type,* DSN: *data_set_name*, REASON: *reason*

Explanation

The data set indicated (*data_set_name*) is not of a type valid for use where it is defined. The reason for the rejection of this data set is found in the REASON field (*reason*).

System action

Processing terminates

User response

Specify a data set of the correct type.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ333E Service *SERVICE FAILED* for *DATA SET*: *dsn - R15: return_code*

Explanation

A z/OS LOCATE or OBTAIN service failed when it was run against the specified data set dsn.

System action

Processing terminates.

User response

Ensure that the data set names exists, and has not been migrated. Determine the cause of the failure by examining the LOCATE/OBTAIN MACRO return codes found in the *IBM DFSMSdfp Advanced Services* manual. Contact IBM Software Support for additional assistance
Parent topic: Error messages and codes: AUIJxxxx

AUIJ335W *dd_name* DD IS PRESENT IN THIS JCL, *dsn_types* WILL NOT BE AUDITED

Explanation

The AUIF*stc* task has encountered a DD in the JCL that prevents a specific type of data set from being audited by SMF.

System action

Accesses to the data set types that are specified in the text of this message are not audited.

User response

If you want to audit accesses to these types of data sets, remove the DD statement. See the Data sets and DD DUMMY statements table in the SMF records section of this user's guide for information on which DDs affect which data set types.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ400E INSUFFICIENT MEMORY - MODULE NAME: *program_name* - MEMORY SEGMENT TYPE: *seg_type*

Explanation

An attempt at obtaining memory in program (*module_name*) has failed due to insufficient memory being available.

System action

Processing terminates

User response

Increase the region size of the started task where this message appeared. Restart the started task and retry the request.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ401E MODULE *module_name* FAILED DURING ATTACH of *program_name* - RETURN CODE: *return_code*

Explanation

An attempt to perform a z/OS® ATTACH of the program_name by module module_name has failed.

System action

Processing terminates.

User response

Determine the cause of the failure by using the return code (*return_code*) provided. Correct and restart the task that issued the message. Contact IBM® Software Support for further assistance if need.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ402E CATALOG SERVICE REQUEST FAILED - MODULE NAME: *module_name* - RC: *return_code* RSN: *reason_code*

Explanation

An attempt use the catalog interface has failed.

System action

Processing terminates

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ403E DYNAMIC ALLOCATION FAILURE - FUNCTION : *function_code* - DSN: *data-set-name* - RC: *return_code* RSN: *reason_code*

Explanation

An attempt to issue a dynamic allocation function (*function_code*) using the data set name indicated (*data_set_name*) has failed.

System action

Processing terminates.

User response

Using the *return_code* and *reason_code* determine the cause for the failure. Correct and retry the request.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ404E DYNAMIC ALLOCATION FAILURE - FUNCTION: *function_code* -DDN: *dd_name* - RC: *return_code* RSN: *reason_code*

Explanation

An attempt to issue a dynamic allocation function (*function_code*) using the DD name indicated (*dd_name*) has failed.

System action

Processing terminates.

User response

Using the *return_code* and *reason_code* determine the cause for the failure. Correct and retry the request.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ406W TOO MANY RULES SPECIFIED IN POLICY, REQUEST HAS BEEN TRUNCATED. POLICY: *policy_name*. RULE LIMIT: *max_number_of rules_allowed*

Explanation

Preprocessing of the rules associated with the indicated policy (*policy_name*) determined that the number of rules that were specified in the policy exceeded the rule limit of *max_number_of rules_allowed*. Allowing an excessive number of rules causes memory constraint and performance issues.

System action

The contents of subsequent rules are discarded. Processing continues using all previous rule content.

User response

Review the rules that are included in the policy, and edit the policy to combine the rule content where permissible. If the resulting policy still requires a greater number of rules than the rule limit permits, contact IBM Software Support.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ407I *number* DATA SETS ADDED TO POLICY *policy_name* FILTER

Explanation

This message provides the number of data set names that are used as input when building the compiled filter for SMF processing.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ408E POLICY *name* RESULTED IN OVER 102400 DATA SETS TO BE AUDITED; DATA SET RESULT SET HAS BEEN TRUNCATED

Explanation

The specified policy has found over 102,400 data sets to audit based on the databases that are specified in the policy rules and the IMS system log data set (SLDS) and recovery log data set (RLDS) RECON entries. Due to memory constraints, the data set occurrence limit per policy is 102,400 per IMS definition.

System action

Remaining data set names for the database description (DBD) that is being processed are included in the list to be audited, which might cause the 102,400 data set limit to be slightly exceeded. The process that determines the DBD and DSN pairings ends, no additional rules within the policy are processed, and a filter is created for the policy based on the 102,400 (or more) data set names. Normal processing continues.

User response

- Change the policy rules to audit fewer databases, or modify the rules to reduce or avoid multiple rules from auditing the same databases.
- Review the IMS RECON data set that is looking for IMS SLDS and RLDS, database image copy data sets, or database data set group (DSG)/area data sets, which no longer physically exist but remain listed in the RECON. Delete the RECON references that are no longer needed.

Parent topic: Error messages and codes: AUIJxxxx

AUIJ500I STARTING *cycle_type* CYCLE

Explanation

The task is starting the processing cycle specified.

System action

Processing starts for the cycle specified.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ501I NO NEW CATALOGED SMF DATA SETS FOUND FOR SMF MASK: - *smf_mask_value*

Explanation

The SMF processing cycle has determined that no new, unprocessed data sets which meet the SMF mask value have been found.

System action

The task waits for the start of the next cycle.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ504I *cycle_type* CYCLE COMPLETE

Explanation

The cycle has completed.

System action

The task waits for the start of the next cycle.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ521W CONTROL BLOCK AUIDCCOM NOT FOUND

Explanation

A critical E/CSA control block was not found.

System action

Processing terminates.

User response

Contact Software Support.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ510I ALTERNATE RECON DATA SETS FOUND FOR IMSNAME *imsname*: RECON1: *alt_dsn_1*; RECON2: *alt_dsn_2*, RECON3: *alt_dsn_3*

Explanation

The AUIARCN DD was found in the JCL. The *imsname* that was used when installing the active IMS policy was found in the AUIARCN file, along with alternate RECON data sets names (*alt_dsn_1/2/3*).

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ511E ALTERNATE RECON DATA SET NOT CATALOGED; DSN: *alt_dsn*

Explanation

When attempting to validate the *alt_dsn* value, the data set was not found in the catalog.

System action

Processing continues to validate other specified data set names.

User response

Correct the data set name or catalog the data set.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ512E ALTERNATE RECON DATA SET NOT A VSAM FILE; DSN: *alt_dsn*

Explanation

When attempting to validate the *alt_dsn* value, the data set was found to in a format invalid for processing. The data set name must be in VSAM format.

System action

Processing continues to validate other specified data set names.

User response

Correct the data set name or catalog the data set.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ513E NO VALID ALTERNATE RECON DATA SETS FOUND FOR IMS *imsname*; PROCESSING TERMINATED

Explanation

The data set validation was completed, and no valid alternate RECON data set names found for the IMSNAME.

System action

Processing terminates.

User response

Add or correct valid RECON data set names.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ522E INSUFFICIENT E/CSA STORAGE AVAILABLE FOR *control_block* CONTROL BLOCK

Explanation

Insufficient E/CSA storage was available to hold the specified control block.

System action

Processing terminates.

User response

Determine the cause of the E/CSA shortage.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ609I *event_types* ARE BEING EXCLUDED (*excluded_by*)

Explanation

If the *excluded_by* value is AGENT, then the reporting of *event_types* is excluded due to the specification of certain configuration keywords. If the *excluded_by* value is IMS, these events are excluded as directed by the IMS definition.

System action

Occurrences of these event types are not reported.

User response

If you want to view reports of this event type, review and modify the agent configuration file (SMF_AUDIT_LEVELS or IMSL_AUDIT_LEVELS keywords) or the Guardium system IMS definition, using the Auditing Levels tab.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ800E REQUIRED DD STATEMENT IS MISSING: *dd-name*

Explanation

A critical error has occurred due to a missing DD statement.

System action

Processing terminates.

User response

This message occurs if a product JCL has been edited and a DD statement has been deleted or omitted. If this is not the case, check for any dynamic allocation error messages. If none are present, or are not user resolvable, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ860E VSAM FILE DEFINITION ERROR - DDN: *dd_name* - REASON: *definition_error*

Explanation

When validating the VSAM repository, an allocation definition error was found.

System action

Processing terminates.

User response

The VSAM repository requires specific values for the attribute, LRECL, key length and key position. Review the SAUISAMP product distribution data set member AUISJ001 for the correct file definition specifications.
Parent topic: Error messages and codes: AUIJxxxx

AUIJ999E AN INTERNAL LOGIC ERROR HAS OCCURRED - MODULE: module_name RSN: reason_code

Explanation

An internal logic error has occurred.

System action

Processing terminates

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIJxxxx

Error messages and codes: AUILxxxx

The following information is about error messages and codes that begin with AUIL.

- **AUIL002I**
  Archive log reader interval set to *<number> <time interval in hours/minutes>*.
- **AUIL003E**
  Command *<command-text>*failed; interval value must be between *<lower-bound>* and *<upper-bound>*.
- **AUIL600I**
  NO NEW CATALOGED IMS LOG DATA SETS FOUND
- **AUIL601I**
  PROCESSING IMS LOG DATA SET: *ims_log_data_set_name*
- **AUIL602I**
  PROCESSING COMPLETE FOR IMS LOG DATA SET: *ims_log_data_set_name*
- **AUIL603I**
  SCANNING RECON DATA SETS FOR IMS LOGS TO PROCESS. RECON1: *recon1_dsn* - RECON2: *recon2_dsn* - RECON3: *recon3_dsn*
- **AUIL605I**
  RECON DATA SET SCAN COMPLETE
- **AUIL606W**
  RECON HAS NOCATDS SPECIFIED, RESULTS MAY NOT BE ACCURATE
- **AUIL607W**
  THERE ARE NO ACTIVE IMS POLICIES FOR AGENT *agent_name*
- **AUIL701I**
  IMS LOG CHECKPOINT INFORMATION - IMSID: *IMS_name_from_policy* - RECON1 DSN: *dsn_of_RECON1* - CREATING SSID: *SSID_from_PRILOG* - LAST DSN READ: *dsn_of_SLDS* - LAST UPDATED (UTC): *date_time*

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIL002I Archive log reader interval set to *<number> <time interval in hours/minutes>*.

Explanation

The Archive log reader is scheduled to process archive logs as specified.

User response

No action is required.
Parent topic: Error messages and codes: AUILxxxx

AUIL003E Command *<command-text>*failed; interval value must be between *<lower-bound>* and *<upper-bound>*.

Explanation

This message indicates that *<command>*, such as: /f AUILSTC,SET INTERVAL number failed because of incorrect *number* value. Correct values must be between *<lower-bound>* and *<upper-bound>*.

User response

Use an interval value between *<lower-bound>* and *<upper-bound>*. If that does not resolve the issue, contact IBM® Software Support.
Parent topic: Error messages and codes: AUILxxxx

AUIL600I NO NEW CATALOGED IMS LOG DATA SETS FOUND

Explanation

After examining the RECON data sets, it has been determined that no new IMS SLDS data sets were found that have yet to be processed by the product.

User response

No action is required.
Parent topic: Error messages and codes: AUILxxxx

AUIL601I PROCESSING IMS LOG DATA SET: *ims_log_data_set_name*

Explanation

Processing has started for the IMS SLDS data set indicated (*ims_log_data_set_name*)

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUILxxxx

AUIL602I PROCESSING COMPLETE FOR IMS LOG DATA SET: *ims_log_data_set_name*

Explanation

Processing of the IMS SLDS data set has completed.

System action

Processing continues with other candidate IMS SLDS data sets.

User response

No action is required.
Parent topic: Error messages and codes: AUILxxxx

AUIL603I SCANNING RECON DATA SETS FOR IMS LOGS TO PROCESS. RECON1: *recon1_dsn* - RECON2: *recon2_dsn* - RECON3: *recon3_dsn*

Explanation

To determine the candidate IMS SLDS data sets to be read, the IMS RECON data sets must be queried. This message indicates that this query process has started.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUILxxxx

AUIL605I RECON DATA SET SCAN COMPLETE

Explanation

This message follows the AUIL603I message and indicates that the scan of the RECON data sets is complete.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUILxxxx

AUIL606W RECON HAS NOCATDS SPECIFIED, RESULTS MAY NOT BE ACCURATE

Explanation

When examining the RECON data sets the NOCATDS option was found to be on, meaning any log data sets found might not be cataloged.

System action

Processing continues.

User response

The function that produces this message relies on the log data sets existing in the z/OS® catalog or having been in the z/OS catalog at one time. Having the NOCATDS option on in the RECON data sets might negate the validity of further processing, if the SLDS data sets are not cataloged.
Parent topic: Error messages and codes: AUILxxxx

AUIL607W THERE ARE NO ACTIVE IMS POLICIES FOR AGENT *agent_name*

Explanation

A request to query the RECON data sets of IMS systems defined under the named agent found that there were no IMS systems audited by the agent with an active profile. The function that produces this message relies on having at least one IMS system with an active collection policy.

System action

Processing terminates.

User response

Install a collection policy for an IMS under of the control the agent.
Parent topic: Error messages and codes: AUILxxxx

AUIL701I IMS LOG CHECKPOINT INFORMATION - IMSID: *IMS_name_from_policy* - RECON1 DSN: *dsn_of_RECON1* - CREATING SSID: *SSID_from_PRILOG* - LAST DSN READ: *dsn_of_SLDS* - LAST UPDATED (UTC): *date_time*

Explanation

This message provides the name of the IMS SLDS that was last read when processing data for the SSID (*SSID_from_PRILOG*) found in the set of the DBRC RECON data sets (*dsn_of_RECON1*). This information is used as a checkpoint to indicate which SLDS data sets have already been processed, and should not be re-read by the AUILstc tasks.

System action

Processing continues.

User response

No action is required.
Parent topic: Error messages and codes: AUILxxxx

Error messages and codes: AUIPxxxx

The following information is about error messages and codes that begin with AUIP.

- **AUIP001E**
  A protobuf message schema violation was detected; value *value* is not a valid boolean value.
- **AUIP002E**
  A protobuf message schema violation was detected; value *value* is not a valid double value.
- **AUIP003E**
  A protobuf message schema violation was detected; value *value* is not a valid integer value.
- **AUIP004E**
  A protobuf message schema violation was detected; required message *message* property *property* is not present.
- **AUIP005E**
  A protobuf message schema violation was detected; required message *message* sub-message *submessage* is not present.
- **AUIP006S**
  A severe error occurred during protobuf message parsing; an unknown exception occurred.
- **AUIP007E**
  A protobuf message schema violation was detected; property name *property* is invalid.
- **AUIP008E**
  A protobuf message schema violation was detected; property *property* value *value* is invalid.
- **AUIP009E**
  A protobuf message schema violation was detected; message name 'name' is invalid.
- **AUIP010E**
  A protobuf message schema violation was detected; message name *name* is invalid (expected *expected name*).
- **AUIP011E**
  A protobuf message schema violation was detected; value *value* is not a valid bytes value.
- **AUIP012E**
  A protobuf message schema violation was detected; value *value* is not a valid unsigned integer value.
- **AUIP013E**
  An error occurred while parsing item text: String is empty.
- **AUIP014E**
  An error occurred while parsing item text: text.
- **AUIP015E**
  Failed to send error message to appliance: *host/port*.
- **AUIP016E**
  Policy rule <rule> was ignored: IMS name is empty.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIP001E A protobuf message schema violation was detected; value *value* is not a valid boolean value.

Explanation

The specified value is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP002E A protobuf message schema violation was detected; value *value* is not a valid double value.

Explanation

The specified value is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP003E A protobuf message schema violation was detected; value *value* is not a valid integer value.

Explanation

The specified value is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP004E A protobuf message schema violation was detected; required message *message* property *property* is not present.

Explanation

The specified message property is not present.

User response

Contact your administrator or IBM® Software Support
Parent topic: Error messages and codes: AUIPxxxx

AUIP005E A protobuf message schema violation was detected; required message *message* sub-message *submessage* is not present.

Explanation

The specified message submessage is not present.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP006S A severe error occurred during protobuf message parsing; an unknown exception occurred.

Explanation

An error occurred while parsing a protobuf message.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP007E A protobuf message schema violation was detected; property name *property* is invalid.

Explanation

The specified property name is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP008E A protobuf message schema violation was detected; property *property* value *value* is invalid.

Explanation

The specified property value is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP009E A protobuf message schema violation was detected; message name 'name' is invalid.

Explanation

The specified message name is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP010E A protobuf message schema violation was detected; message name *name* is invalid (expected *expected name*).

Explanation

The specified message name is not valued.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP011E A protobuf message schema violation was detected; value *value* is not a valid bytes value.

Explanation

The specified value is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP012E A protobuf message schema violation was detected; value *value* is not a valid unsigned integer value.

Explanation

The specified value is not valid.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP013E An error occurred while parsing item text: String is empty.

Explanation

A policy message contained an item field with an empty value.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP014E An error occurred while parsing item text: text.

Explanation

A policy message contained an item field with a value *text* could not be parsed successfully.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP015E Failed to send error message to appliance: *host/port*.

Explanation

The IBM® Guardium® S-TAP® for IMS agent was unable to send the error message to the specified appliance.

User response

Contact your administrator or IBM Software Support.
Parent topic: Error messages and codes: AUIPxxxx

AUIP016E Policy rule <rule> was ignored: IMS name is empty.

Explanation

The specified policy rule was ignored because it does not apply to any IMS subsystem, or the IMS name is empty.

User response

Contact your administrator or IBM® Software Support.
Parent topic: Error messages and codes: AUIPxxxx

Error messages and codes: AUIRxxxx

The following information is about error messages and codes that begin with AUIR.

- **AUIR002E**
  The provided *parameter 'value'* is too long; should be less than or equal to *maximum length* characters.
- **AUIR004E**
  A maximum of *maximum* data sets are allowed for the *names* libs and a total of *libs-count* were specified.
- **AUIR006E**
  The parameter *parameter* can't be empty.
- **AUIR007W**
  Policy_rule_item *<item-name>* for Policy_rule *<rule-name>* has conflicting *<value-name>* values.
- **AUIR008W**
  IMS 050i Max Time threshold was changed from "2460" to "2359".

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIR002E The provided *parameter 'value'* is too long; should be less than or equal to *maximum length* characters.

Explanation

The value of the specified *parameter* exceeds the maximum length *maximum length*.

User response

Specify a shorter value that does not exceed the specified limit for the parameter.
Parent topic: Error messages and codes: AUIRxxxx

AUIR004E A maximum of *maximum* data sets are allowed for the *names* libs and a total of *libs-count* were specified.

Explanation

The maximum number of data sets was exceeded for the libs specified.

User response

Limit the number of data sets for the specified libs to *maximum*.
Parent topic: Error messages and codes: AUIRxxxx

AUIR006E The parameter *parameter* can't be empty.

Explanation

The parameter value must be specified in the agent configuration.

User response

Update agent configuration, or contact your administrator.
Parent topic: Error messages and codes: AUIRxxxx

AUIR007W Policy_rule_item *<item-name>* for Policy_rule *<rule-name>* has conflicting *<value-name>* values.

Explanation

The Guardium policy was processed but there are conflicting fields in the definition. Only one of the policies has been applied.

User response

Check the policy definition, and change the specified values to eliminate the conflict.
Parent topic: Error messages and codes: AUIRxxxx

AUIR008W IMS 050i Max Time threshold was changed from "2460" to "2359".

Explanation

An invalid time value was supplied through the use of the Message AUII050I Frequency field of the IMS definition screen of the Guardium® appliance. The invalid value was automatically corrected by the agent.

System action

Processing continues.

User response

When convenient, update the invalid time value in the IMS definition to a value within the range of 00:10 -- 23:59.
Parent topic: Error messages and codes: AUIRxxxx

Error messages and codes: AUITxxxx

The following information is about error messages and codes that begin with AUIT.

- **AUIT001E**
  The specified user ID *userid* is not defined or does not have an OMVS segment defined.
- **AUIT006S**
  The product is not properly configured to authenticate users.
- **AUIT008E**
  The configuration file *filename* is invalid; the root element *element* is not <agent-config>.
- **AUIT010E**
  An error occurred while opening the configuration file *filename message text*
- **AUIT012I**
  Performing discovery of available locations.
- **AUIT013I**
  Security Guardium® S-TAP® for IMS agent is terminating.
- **AUIT014I**
  Connected to server *<host>* on port *<port>*.
- **AUIT015I**
  Attempting connection to server *<host>* on port *<port>*.
- **AUIT017I**
  Discovered subsystem *subsystem-id*.
- **AUIT019I**
  Security Guardium S-TAP for IMS agent started on *<lpar _name> (<lpar_ip>)*.
- **AUIT020I**
  Starting the socket selector thread (thread *thread id*).
- **AUIT023I**
  Received shutdown request.
- **AUIT025I**
  The socket selector thread is terminating.
- **AUIT028E**
  An error occurred while authenticating user *user-id error-text*.
- **AUIT031I**
  Starting the command listener thread (thread *thread-id*).
- **AUIT032I**
  Received stop command: *command-text*.
- **AUIT033I**
  Received modify command: *command-text*.
- **AUIT034S**
  Security Guardium S-TAP for IMS agent is terminating due to hard stop request.
- **AUIT044E**
  The connection to the server has been lost.
- **AUIT047E**
  IBM® Security Guardium S-TAP for IMS on z/OS® agent ended with RC = *[rc]*.
- **AUIT048I**
  Issuing request to capture service dump.
- **AUIT049I**
  Request to capture service dump has completed successfully.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIT001E The specified user ID *userid* is not defined or does not have an OMVS segment defined.

Explanation

You specified a user ID that is not defined or does not have an OMVS segment defined.

User response

Security Guardium® S-TAP® for IMS was unable to authenticate the specified user. Either specify a valid user ID, or if the user ID is valid, see your security administrator to have an OMVS segment defined for the user ID.

Parent topic: Error messages and codes: AUITxxxx

AUIT006S The product is not properly configured to authenticate users.

Explanation

Security Guardium® S-TAP® for IMS is not properly configured to authenticate users.

User response

An error occurred while authenticating a remote user request. The error code indicates that the installation configuration required to allow this authentication has not been completed. See IBM Guardium S-TAP for IMS agent for more information about how to complete the required configuration.
Parent topic: Error messages and codes: AUITxxxx

AUIT008E The configuration file *filename* is invalid; the root element *element* is not <agent-config>.

Explanation

The configuration file identified in the message is invalid.

User response

The contents of the specified configuration file are invalid. Correct the file contents to specify <agent-config> as the root XML element.

Parent topic: Error messages and codes: AUITxxxx

AUIT010E An error occurred while opening the configuration file *filename message text*

Explanation

An error occurred while opening the configuration file identified in the message. Additional error information is also contained within the message.

User response

Use the specified message text to diagnose the error that occurred. Specify a valid configuration file that is not in use by any other process.

Parent topic: Error messages and codes: AUITxxxx

AUIT012I Performing discovery of available locations.

Explanation

The Security Guardium® S-TAP® for IMS agent is looking for available locations.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT013I Security Guardium® S-TAP® for IMS agent is terminating.

Explanation

The Security Guardium S-TAP for IMS agent is terminating.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT014I Connected to server *<host>* on port *<port>*.

Explanation

The Security Guardium® S-TAP® for IMS agent task has connected to the S-TAP to the specified host and port.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT015I Attempting connection to server *<host>* on port *<port>*.

Explanation

The Security Guardium® S-TAP® for IMS agent is attempting to connect to the specified host and port number.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT017I Discovered subsystem *subsystem-id*.

Explanation

The Security Guardium® S-TAP® for IMS agent has discovered the identified subsystem.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT019I Security Guardium® S-TAP® for IMS agent started on *<lpar _name> (<lpar_ip>)*.

Explanation

The IBM® Guardium S-TAP for IMS agent has started.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT020I Starting the socket selector thread (thread *thread id*).

Explanation

The Security Guardium® S-TAP® for IMS agent is starting the identified socket selector thread.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT023I Received shutdown request.

Explanation

The Security Guardium® S-TAP® for IMS agent has received a shutdown request.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT025I The socket selector thread is terminating.

Explanation

The Security Guardium® S-TAP® for IMS agent socket selector thread is terminating.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT028E An error occurred while authenticating user *user-id error-text*.

Explanation

An unexpected return code was returned by the *pthread_security_np()* callable service.

User response

Ensure that the configuration required to use this service has been completed. See IBM Guardium S-TAP for IMS agent for more information about the required configuration. Check the agent job log for additional messages which might be generated.

Parent topic: Error messages and codes: AUITxxxx

AUIT031I Starting the command listener thread (thread *thread-id*).

Explanation

The Security Guardium® S-TAP® for IMS agent is starting the command listener thread.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT032I Received stop command: *command-text*.

Explanation

The Security Guardium® S-TAP® for IMS agent received a STOP command.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT033I Received modify command: *command-text*.

Explanation

The Security Guardium® S-TAP® for IMS agent received a MODIFY command.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT034S Security Guardium® S-TAP® for IMS agent is terminating due to hard stop request.

Explanation

Security Guardium S-TAP for IMS agent is terminating due to a user /MODIFY FORCE command.

User response

No action is required.

Parent topic: Error messages and codes: AUITxxxx

AUIT044E The connection to the server has been lost.

Explanation

The Security Guardium® S-TAP® for IMS agent task is unable to communicate with the Security Guardium S-TAP for IMS agent.

User response

Resolve any network connectivity issues, then try logging in again.
Parent topic: Error messages and codes: AUITxxxx

AUIT047E IBM® Security Guardium® S-TAP® for IMS on z/OS® agent ended with RC = *[rc]*.

Explanation

Due to a prior error, the agent has ended with the specified return code.

User response

Contact IBM Software Support.
Parent topic: Error messages and codes: AUITxxxx

AUIT048I Issuing request to capture service dump.

Explanation

A command, such as /f AUIASTC,DUMP/DDX, has been issued for processing.

User response

No action is required.
Parent topic: Error messages and codes: AUITxxxx

AUIT049I Request to capture service dump has completed successfully.

Explanation

A command, such as /f AUIASTC,DUMP/DDX has processed successfully.

User response

No action is required.
Parent topic: Error messages and codes: AUITxxxx

Error messages and codes: AUIUxxxx

The following information is about error messages and codes that begin with AUIU.

- **AUIUR002I**
  Migrate Utility for IBM® Security Guardium® S-TAP® for IMS on z/OS® started.
- **AUIUR003I**
  Agent record *<agent name>* was not found in the repository.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIUR002I Migrate Utility for IBM® Security Guardium® S-TAP® for IMS on z/OS® started.

Explanation

The utility to migrate the configuration of an older version of the product to the current product version has started.

User response

No action is required.
Parent topic: Error messages and codes: AUIUxxxx

AUIUR003I Agent record *<agent name>* was not found in the repository.

Explanation

An attempt to read an agent record from the repository while migration failed as the record was not found.

System action

The agent record migration fails, processing continues.

User response

Check the configuration file for agent and repository names and use the Guardium user interface to verify that the specified agent definition is presented in specified repository.
Parent topic: Error messages and codes: AUIUxxxx

Error messages and codes: AUIXxxxx

The following information is about error messages and codes that begin with AUIX.

- **AUIX013E**
  A shared memory error occurred on "*service name*": *error message*.
- **AUIX014E**
  An XML schema violation was detected; value *value* is not a valid boolean value.
- **AUIX015E**
  An XML schema violation was detected; value *value* is not a valid double value.
- **AUIX016E**
  An XML schema violation was detected; value *value* is not a valid integer value.
- **AUIX017E**
  An XML syntax error was detected at offset *offset*; expected *expected-value*, found *found-value*.
- **AUIX018E**
  An XML schema violation was detected; required element *element* attribute *attribute*\" is not present.

- **AUIX019E**
  An XML schema violation was detected; required element *<element>* child *<child-element>* is not present.
- **AUIX020E**
  Memory allocation failed (*number* bytes).
- **AUIX021E**
  An XML schema violation was detected; element *element* child *child-number* has wrong type.
- **AUIX022E**
  An XML syntax error was detected; character reference *character-reference* is invalid.
- **AUIX023E**
  An XML syntax error was detected; entity reference *entity-reference* is invalid.
- **AUIX024E**
  An XML syntax error was detected; more than one element was found at the root of the document.
- **AUIX025E**
  An XML syntax error was detected; no element was found at the root of the document.
- **AUIX026E**
  An XML syntax error was detected; text was found at the root of the document.
- **AUIX027S**
  A severe error occurred during XML parsing; an unknown exception occurred.
- **AUIX028E**
  The command line option *<option name>* is invalid.
- **AUIX034S**
  A severe error occurred during command line processing; an unknown exception occurred.
- **AUIX035E**
  The operation completed successfully.
- **AUIX036E**
  The address family is not supported by the protocol family (*socket-return-code*).
- **AUIX037E**
  The operation is still in progress (*socket-return-code*).
- **AUIX038E**
  Permission is denied (*socket-return-code*).
- **AUIX039E**
  The network is down (*socket-return-code*).
- **AUIX040E**
  No buffer space is available (*socket-return-code*).
- **AUIX041E**
  Too many sockets have been opened (*socket-return-code*).
- **AUIX042E**
  The protocol is not supported (*socket-return-code*).
- **AUIX043E**
  The WSAStartup routine was not called (*socket-return-code*).
- **AUIX044E**
  The protocol is the wrong type for the socket (*socket-return-code*).
- **AUIX045E**
  The socket type is not supported (*socket-return-code*).
- **AUIX046E**
  The destination network is unreachable (*socket-return-code*).
- **AUIX047E**
  The socket handle is invalid (*socket-return-code*).
- **AUIX048E**
  The address is already in use (*socket-return-code*).
- **AUIX049E**
  The function call was interrupted (*socket-return-code*
- **AUIX050E**
  The requested address is not available (*socket-return-code*).
- **AUIX051E**
  The connection was aborted (*socket-return-code*).
- **AUIX052E**
  The connection was refused by the partner (*socket-return-code*).
- **AUIX053E**
  The connection was reset by the partner (*socket-return-code*).
- **AUIX054E**
  The network message is too long (*socket-return-code*).
- **AUIX055E**
  The network dropped the connection when reset (*socket-return-code*).
- **AUIX056E**
  An invalid parameter was specified (*socket-return-code*).
- **AUIX057E**
  The socket is not connected (*socket-return-code*).
- **AUIX058E**
  The operation is not supported (*socket-return-code*).
- **AUIX059E**
  The socket has been closed (*socket-return-code*).
- **AUIX060E**
  The socket is already connected (*socket-return-code*).
- **AUIX061S**
  An unknown error occurred (*socket-return-code*).
- **AUIX062E**
  A socket error occurred on *socket-operation* with RC = *return code*: *message-text*.
- **AUIX063E**
  A socket select error occurred: *message-text*.

- **AUIX064E**
  An XML schema violation was detected; expected root element *element-expected*, but found *element-found* instead.
- **AUIX066E**
  An XML schema violation was detected; element *element* value *value* is invalid.
- **AUIX067E**
  An XML schema violation was detected; element name *element* is invalid.
- **AUIX068E**
  An XML schema violation was detected; element name *element-found* is invalid (expected *element-expected*).
- **AUIX074E**
  An abend occurred: *<abend code>*.
- **AUIX076E**
  An XML schema violation was detected; element *element* attribute *attribute* value *value* is invalid.
- **AUIX085E**
  A dynamic allocation error occurred: info code = *info-code*, error code = *error-code*.
- **AUIX086E**
  A dynamic concatenation error occurred: info code = *info-code*, error code = *error-code*.
- **AUIX087E**
  A dynamic free error occurred: info code = *info-code*, error code = *error-code*.
- **AUIX088E**
  An invalid dynamic allocation parameter was specified: code = *parm-code*.
- **AUIX093S**
  An unexpected error occurred (*file-name*, *line-number*).
- **AUIX094S**
  An unexpected error occurred with token *token*, (*file-name*, *line-number*).
- **AUIX095S**
  An unexpected error occurred with tokens *token* and *token* (*file-name*, *line-number*).
- **AUIX096S**
  An unexpected error occurred with tokens *token*, *token* and *token* (*file-name*, *line-number*).
- **AUIX097S**
  An unexpected error occurred with tokens *token*, *token*, *token*, and *token* (*file-name*, *line-number*.
- **AUIX098E**
  A thread error occurred on *thread-operation* : *message-text*.
- **AUIX101E**
  An event error occurred on *event-operation* : *message-text*.
- **AUIX104E**
  A mutex error occurred on *mutex-operation* : *message-text*.
- **AUIX109E**
  A semaphore error occurred on *semaphore-operation* : *message-text*.
- **AUIX110I**
  The network connection has been disconnected.
- **AUIX114E**
  A dynamic allocation query error occurred: info code = *info-code*, error code = *error-code*.
- **AUIX115E**
  An input command error occurred on \"*command-operation*\": *message-text*.
- **AUIX116I**
  Received input command: *command-text*.
- **AUIX122I**
  Build date *component* = *date*.
- **AUIX123W**
  The action was cancelled.
- **AUIX124S**
  The task is not running APF-authorized.
- **AUIX126E**
  A DLL error occurred on *dll-operation* : *message-text*
- **AUIX127S**
  An error occurred while opening log file *file-name*.
- **AUIX142E**
  An XML schema violation was detected; element *element* value *value* is invalid: expected min *<min-value>* and max *<max value>*.
- **AUIX143E**
  An XML schema violation was detected; element *element* attribute *value* value *value* is invalid: expected min *<minimum>* and max *<maximum>*.
- **AUIX149E**
  Data set *[data set]* is not cataloged.
- **AUIX150E**
  Invalid data set *'data set'*: Data set name must not exceed 44 characters.
- **AUIX151E**
  Invalid data set *{'data set'}*: The segment length must be greater than 0 and less than or equal to 8.
- **AUIX152E**
  Invalid data set *'name'*: The first character in each segment must be alphabetic (A-Z) or national (#, @, $).
- **AUIX153E**
  Invalid data set *'<data set>'*: The non-first characters in the segments must be alphabetic (A-Z), numeric, national (#, @, $), or hyphen.
- **AUIX154E**
  Invalid data set *'<data set>'*: The non-first characters in the SMF segments must be alphabetic (A -- Z), numeric, national (#, @, $), hyphen, asterisk (*) or percent (%).
- **AUIX155E**
  Data set *<data set>* is not APF-authorized.
- **AUIX156E**
  Invalid data set *'<data set>'*: The first character in SMF segment must be alphabetic (A -- Z) or national (#, @, $), asterisk (*) or percent (%).
- **AUIX160E**
  A dynamic allocation query error occurred: info code = *<info-code>*, error code = *<error-code>*, DD name = *<dd-name>*.

- **AUIX183E**
  The number of file descriptors (sockets) has exceeded maximum = <*number*>.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIX013E A shared memory error occurred on "*service name*": *error message*.

Explanation

This error can occur in the primary agent address space. When the error occurs, the primary agent address space will shut down with a CC of 12. This startup error indicates that attempts to create a shared memory segment failed because of an already existing shared memory segment that never belonged to, or currently does not belong to, the primary agent address space.

This message can occur in the secondary address space if the <id> elements in the ADS_SHM_ID and ADS_LISTENER_PORT parameters do not match in the AUICONFG configuration member that is used by the agent primary address space and the secondary address spaces.

User response

Edit SAUISAMP member AUICONFG (or the customized AUICONFG) and specify the correct <id> elements in the ADS_SHM_ID and ADS_LISTENER_PORT parameters.
Parent topic: Error messages and codes: AUIXxxxx

AUIX014E An XML schema violation was detected; value *value* is not a valid boolean value.

Explanation

An XML schema violation was detected; value value is not a valid boolean value.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX015E An XML schema violation was detected; value *value* is not a valid double value.

Explanation

An XML schema violation was detected; value *value* is not a valid double value.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX016E An XML schema violation was detected; value *value* is not a valid integer value.

Explanation

An XML schema violation was detected; value value is not a valid integer value.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX017E An XML syntax error was detected at offset *offset*; expected *expected-value*, found *found-value*.

Explanation

An XML syntax error was detected at offset offset; expected expected-value, found found-value.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX018E An XML schema violation was detected; required element *element* attribute *attribute*\" is not present.

Explanation

An XML schema violation was detected; required element element attribute attribute is not present.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX019E An XML schema violation was detected; required element *<element>* child *<child-element>* is not present.

Explanation

The XML schema must contain the specified elements.

User response

Correct the XML schema and retry.
Parent topic: Error messages and codes: AUIXxxxx

AUIX020E Memory allocation failed (*number* bytes).

Explanation

Memory allocation failed (number bytes).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX021E An XML schema violation was detected; element *element* child *child-number* has wrong type.

Explanation

An XML schema violation was detected; element element child child-number has wrong type.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX022E An XML syntax error was detected; character reference *character-reference* is invalid.

Explanation

An XML syntax error was detected; character reference character-reference is invalid.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX023E An XML syntax error was detected; entity reference *entity-reference* is invalid.

Explanation

An XML syntax error was detected; entity reference entity-reference is invalid.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX024E An XML syntax error was detected; more than one element was found at the root of the document.

Explanation

An XML syntax error was detected; more than one element was found at the root of the document.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX025E An XML syntax error was detected; no element was found at the root of the document.

Explanation

An XML syntax error was detected; no element was found at the root of the document.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX026E An XML syntax error was detected; text was found at the root of the document.

Explanation

An XML syntax error was detected; text was found at the root of the document.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX027S A severe error occurred during XML parsing; an unknown exception occurred.

Explanation

A severe error occurred during XML parsing; an unknown exception occurred.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX028E The command line option *<option name>* is invalid.

Explanation

The command line option, which is specified in the message text, is invalid.

User response

Correct the command line option and retry the operation. Review the IBM® Guardium® S-TAP® for IMS client/server environment information for valid options.

Parent topic: Error messages and codes: AUIXxxxx

AUIX034S A severe error occurred during command line processing; an unknown exception occurred.

Explanation

A severe error occurred during command line processing; an unknown exception occurred.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX035E The operation completed successfully.

Explanation

The operation completed successfully.

User response

No action is required.

Parent topic: Error messages and codes: AUIXxxxx

AUIX036E The address family is not supported by the protocol family (*socket-return-code*).

Explanation

The address family is not supported by the protocol family (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX037E The operation is still in progress (*socket-return-code*).

Explanation

The operation is still in progress (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX038E Permission is denied (*socket-return-code*).

Explanation

Permission is denied (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX039E The network is down (*socket-return-code*).

Explanation

The network is down (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX040E No buffer space is available (*socket-return-code*).

Explanation

No buffer space is available (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX041E Too many sockets have been opened (*socket-return-code*).

Explanation

Too many sockets have been opened (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX042E The protocol is not supported (*socket-return-code*).

Explanation

The protocol is not supported (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX043E The WSAStartup routine was not called (*socket-return-code*).

Explanation

The WSAStartup routine was not called (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX044E The protocol is the wrong type for the socket (*socket-return-code*).

Explanation

The protocol is the wrong type for the socket (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX045E The socket type is not supported (*socket-return-code*).

Explanation

The socket type is not supported (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX046E The destination network is unreachable (*socket-return-code*).

Explanation

The destination network is unreachable (socket-return-code).

User response

Specify the correct host name or IP address.

Parent topic: Error messages and codes: AUIXxxxx

AUIX047E The socket handle is invalid (*socket-return-code*).

Explanation

The socket handle is invalid (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX048E The address is already in use (*socket-return-code*).

Explanation

The address is already in use (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX049E The function call was interrupted (*socket-return-code*

Explanation

The function call was interrupted (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX050E The requested address is not available (*socket-return-code*).

Explanation

The requested address is not available (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX051E The connection was aborted (*socket-return-code*).

Explanation

The connection was aborted (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX052E The connection was refused by the partner (*socket-return-code*).

Explanation

The connection was refused by the partner (socket-return-code).

User response

Verify that the correct port number was specified, and that the partner application has been started and is available.

Parent topic: Error messages and codes: AUIXxxxx

AUIX053E The connection was reset by the partner (*socket-return-code*).

Explanation

The connection was reset by the partner (socket-return-code).

User response

The partner application ended the network connection. If this is unexpected, diagnose the partner application failure. Otherwise, no action is required.

Parent topic: Error messages and codes: AUIXxxxx

AUIX054E The network message is too long (*socket-return-code*).

Explanation

The network message is too long (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX055E The network dropped the connection when reset (*socket-return-code*).

Explanation

The network dropped the connection when reset (socket-return-code

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX056E An invalid parameter was specified (*socket-return-code*).

Explanation

An invalid parameter was specified (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX057E The socket is not connected (*socket-return-code*).

Explanation

The socket is not connected (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX058E The operation is not supported (*socket-return-code*).

Explanation

The operation is not supported (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX059E The socket has been closed (*socket-return-code*).

Explanation

The socket has been closed (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX060E The socket is already connected (*socket-return-code*).

Explanation

The socket is already connected (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX061S An unknown error occurred (*socket-return-code*).

Explanation

An unknown error occurred (socket-return-code).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX062E A socket error occurred on *socket-operation* with RC = *return code*: *message-text*.

Explanation

A socket error occurred.

User response

Use the specified message text to diagnose the error.

Parent topic: Error messages and codes: AUIXxxxx

AUIX063E A socket select error occurred: *message-text*.

Explanation

A socket select error occurred.

User response

Use the specified message text to diagnose the error.

Parent topic: Error messages and codes: AUIXxxxx

AUIX064E An XML schema violation was detected; expected root element *element-expected*, but found *element-found* instead.

Explanation

An XML schema violation was detected; expected root element element-expected , but found element-found instead.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX066E An XML schema violation was detected; element *element* value *value* is invalid.

Explanation

An XML schema violation was detected; element element value value is invalid.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX067E An XML schema violation was detected; element name *element* is invalid.

Explanation

An XML schema violation was detected; element name element is invalid.

User response

If the error occurred while reading the agent configuration file, correct the file contents. Otherwise, contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX068E An XML schema violation was detected; element name *element-found* is invalid (expected *element-expected*).

Explanation

An XML schema violation was detected; element name element-found is invalid (expected element-expected).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX074E An abend occurred: *<abend code>*.

Explanation

This message indicates a callable service abend has occurred. Additional diagnostic information might be present in the message when applicable.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIXxxxx

AUIX076E An XML schema violation was detected; element *element* attribute *attribute* value *value* is invalid.

Explanation

An XML schema violation was detected; element element attribute attribute value value is invalid.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX085E A dynamic allocation error occurred: info code = *info-code*, error code = *error-code*.

Explanation

A dynamic allocation error occurred: info code = info-code, error code = error-code.

User response

See the *MVS™ Programming: Authorized Assembler Services Guide* for more information about the specified information and error codes.

Parent topic: Error messages and codes: AUIXxxxx

AUIX086E A dynamic concatenation error occurred: info code = *info-code*, error code = *error-code*.

Explanation

A dynamic concatenation error occurred: info code = info-code, error code = error-code.

User response

See the *MVS™ Programming: Authorized Assembler Services Guide* for more information about the specified information and error codes.

Parent topic: Error messages and codes: AUIXxxxx

AUIX087E A dynamic free error occurred: info code = *info-code*, error code = *error-code*.

Explanation

A dynamic free error occurred: info code = info-code, error code = error-code.

User response

See the *MVS™ Programming: Authorized Assembler Services Guide* for more information about the specified information and error codes.

Parent topic: Error messages and codes: AUIXxxxx

AUIX088E An invalid dynamic allocation parameter was specified: code = *parm-code*.

Explanation

An invalid dynamic allocation parameter was specified: code = parm-code.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX093S An unexpected error occurred (*file-name*, *line-number*).

Explanation

An unexpected error occurred (file-name, line-number).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX094S An unexpected error occurred with token *token*, (*file-name*, *line-number*).

Explanation

An unexpected error occurred with token token, (file-name, line-number).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX095S An unexpected error occurred with tokens *token* and *token* (*file-name*, *line-number*).

Explanation

An unexpected error occurred with tokens token and token (file-name, line-number).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX096S An unexpected error occurred with tokens *token*, *token* and *token* (*file-name*, *line-number*).

Explanation

An unexpected error occurred with tokens token, token and token (file-name, line-number).

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX097S An unexpected error occurred with tokens *token*, *token*, *token*, and *token* (*file-name*, *line-number*.

Explanation

An unexpected error occurred with tokens token, token, token, and token (file-name, line-number.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX098E A thread error occurred on *thread-operation* : *message-text*.

Explanation

A thread error occurred on thread-operation : message-text.

User response

Use the specified message text to diagnose the error.

Parent topic: Error messages and codes: AUIXxxxx

AUIX101E An event error occurred on *event-operation* : *message-text*.

Explanation

An event error occurred on event-operation : message-text.

User response

Use the specified message text to diagnose the error.

Parent topic: Error messages and codes: AUIXxxxx

AUIX104E A mutex error occurred on *mutex-operation* : *message-text*.

Explanation

A mutex error occurred on mutex-operation : message-text.

User response

Use the specified message text to diagnose the error.

Parent topic: Error messages and codes: AUIXxxxx

AUIX109E A semaphore error occurred on *semaphore-operation* : *message-text*.

Explanation

A semaphore error occurred on semaphore-operation : message-text.

User response

Use the specified message text to diagnose the error.

Parent topic: Error messages and codes: AUIXxxxx

AUIX110I The network connection has been disconnected.

Explanation

The network connection has been disconnected.

User response

No action is required.

Parent topic: Error messages and codes: AUIXxxxx

AUIX114E A dynamic allocation query error occurred: info code = *info-code*, error code = *error-code*.

Explanation

A dynamic allocation query error occurred: info code = info-code, error code = error-code.

User response

See the *MVS™ Programming: Authorized Assembler Services Guide* for more information about the specified info and error codes.

Parent topic: Error messages and codes: AUIXxxxx

AUIX115E An input command error occurred on \"*command-operation*\": *message-text*.

Explanation

An input command error occurred on \"command-operation\": message-text.

User response

Contact IBM® Customer Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX116I Received input command: *command-text*.

Explanation

Received input command: command-text.

User response

No action is required.

Parent topic: Error messages and codes: AUIXxxxx

AUIX122I Build date *component* = *date*.

Explanation

Build date component = date.

User response

No action is required.

Parent topic: Error messages and codes: AUIXxxxx

AUIX123W The action was cancelled.

Explanation

The action was cancelled.

User response

No action is required. The operation was cancelled due to user or administrator request.

Parent topic: Error messages and codes: AUIXxxxx

AUIX124S The task is not running APF-authorized.

Explanation

The task is not running APF-authorized.

User response

The Security Guardium® S-TAP® for IMS load library, and the load libraries for all of the IMS subsystems accessed, must be APF-authorized. See IBM Guardium S-TAP for IMS agent for more information about the required configuration steps.

Parent topic: Error messages and codes: AUIXxxxx

AUIX126E A DLL error occurred on *dll-operation* : *message-text*

Explanation

A DLL error occurred on dll-operation : message-text

User response

Contact IBM® Customer Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX127S An error occurred while opening log file *file-name*.

Explanation

An error occurred while opening log file file-name.

User response

Contact IBM® Customer Support.

Parent topic: Error messages and codes: AUIXxxxx

AUIX142E An XML schema violation was detected; element *element* value *value* is invalid: expected min *<min-value>* and max *<max value>*.

Explanation

The *element-value* given for *element-name* is out of the range and must be within *min-value* and *max-value*.

User response

Correct the value for the *element-name* in the configuration.

Parent topic: Error messages and codes: AUIXxxxx

AUIX143E An XML schema violation was detected; element *element* attribute *value* value *value* is invalid: expected min *<minimum>* and max *<maximum>*.

Explanation

The element attribute value is not valid.

User response

If the error occurred while reading the agent configuration file, update the configuration. Otherwise, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIXxxxx

AUIX149E Data set *[data set]* is not cataloged.

Explanation

The data set specified in the message text has not been cataloged.

User response

Allocate the data set.
Parent topic: Error messages and codes: AUIXxxxx

AUIX150E Invalid data set *'data set'*: Data set name must not exceed 44 characters.

Explanation

MVS™ data sets cannot exceed 44 characters.

User response

Correct the data set entry, then retry.
Parent topic: Error messages and codes: AUIXxxxx

AUIX151E Invalid data set *{'data set'}*: The segment length must be greater than 0 and less than or equal to 8.

Explanation

The specified data set name has one or more segments that are not between 1 and 8 characters.

User response

Specify a data set where each segment contains more than 0 characters and 8 or fewer characters.
Parent topic: Error messages and codes: AUIXxxxx

AUIX152E Invalid data set *'name'*: The first character in each segment must be alphabetic (A-Z) or national (#, @, $).

Explanation

The data set name provided does not is not a valid name and does not satisfy the MVS™ data set naming requirements.

User response

Correct the data set name and try again.
Parent topic: Error messages and codes: AUIXxxxx

AUIX153E Invalid data set *'<data set>'*: The non-first characters in the segments must be alphabetic (A-Z), numeric, national (#, @, $), or hyphen.

Explanation

The non-first characters in the segments must be alphabetic (A-Z), numeric, national (#, @, $), or hyphen.

User response

Specify a data set where non-first characters in the segments is alphabetic (A-Z), numeric, national (#, @, $), or hyphen.
Parent topic: Error messages and codes: AUIXxxxx

AUIX154E Invalid data set '*<data set>*': The non-first characters in the SMF segments must be alphabetic (A -- Z), numeric, national (#, @, $), hyphen, asterisk (*) or percent (%).

Explanation

The non-first characters in the SMF segments must be alphabetic (A -- Z), numeric, national (#, @, $), hyphen, asterisk (*) or percent (%).

User response

Specify a data set where non-first characters in the SMF segments is alphabetic (A -- Z), numeric, national (#, @, $), hyphen, asterisk (*) or percent (%).
Parent topic: Error messages and codes: AUIXxxxx

AUIX155E Data set *<data set>* is not APF-authorized.

Explanation

The specified data set requires APF authorization.

User response

The specified data set must be APF-authorized. See Configuration overview for more information about the required configuration steps.
Parent topic: Error messages and codes: AUIXxxxx

AUIX156E Invalid data set '*<data set>*': The first character in SMF segment must be alphabetic (A -- Z) or national (#, @, $), asterisk (*) or percent (%).

Explanation

The first character in SMF segment must be alphabetic (A -- Z) or national (#, @, $), asterisk (*) or percent (%).

User response

Specify a data set where first character in SMF segments must be alphabetic (A -- Z) or national (#, @, $), asterisk (*) or percent (%).
Parent topic: Error messages and codes: AUIXxxxx

AUIX160E A dynamic allocation query error occurred: info code = *<info-code>*, error code = *<error-code>*, DD name = *<dd-name>*.

Explanation

A dynamic allocation query error occurred with the specified information code, error code, and DD name.

User response

See the *MVS Programming: Authorized Assembler Services Guide* for more information about the specified info and error codes.
Parent topic: Error messages and codes: AUIXxxxx

AUIX183E The number of file descriptors (sockets) has exceeded maximum = *<number>*.

Explanation

The active program holds too many file or socket descriptors and exceeded system maximum = *<number>*.

User response

Contact your system administrator or IBM Software Support.
Parent topic: Error messages and codes: AUIXxxxx

Error messages and codes: AUIYxxxx

The following information is about error messages and codes that begin with AUIY.

- **AUIY001E**
  A callable services abend *abend* has occurred.
- **AUIY002E**
  GPRS *number-number*: *hex-value hex-value hex-value hex-value*
- **AUIY003E**
  Active module not found.
- **AUIY004E**
  Active module = *module-name*, load point = *hex-address*, offset = *hex-address*
- **AUIY005E**
  PSW = *string string*
- **AUIY006E**
  Callable service invocation failed with return code = *return-code* and reason code = *reason-code*
- **AUIY007I**
  Invoking callable service *callable service*.
- **AUIY008I**
  Returned from callable service *service-name*
- **AUIY009E**
  Invalid data set mask: *data set mask*.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIY001E A callable services abend *abend* has occurred.

Explanation

This message indicates a callable service abend has occurred. Additional diagnostic information is be present in the message when applicable.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIYxxxx

AUIY002E GPRS *number-number*: *hex-value hex-value hex-value hex-value*

Explanation

This message indicates an CSI abend has occurred. Additional diagnostic information is present in the message when applicable.

User response

No action is required.
Parent topic: Error messages and codes: AUIYxxxx

AUIY003E Active module not found.

Explanation

This message indicates a CSI abend has occurred. Additional diagnostic information is present in the message when applicable.

User response

No action is required.
Parent topic: Error messages and codes: AUIYxxxx

AUIY004E Active module = *module-name*, load point = *hex-address*, offset = *hex-address*

Explanation

This message indicates a CSI abend has occurred. Additional diagnostic information is present in the message when applicable.

User response

No action is required.
Parent topic: Error messages and codes: AUIYxxxx

AUIY005E PSW = *string string*

Explanation

This message indicates a CSI abend has occurred. Additional diagnostic information is present in the message when applicable.

User response

No action is required.
Parent topic: Error messages and codes: AUIYxxxx

AUIY006E Callable service invocation failed with return code = *return-code* and reason code = *reason-code*

Explanation

A service requested by the agent task has failed.

User response

View the JES log of the agent task to determine the data set name and reason for the error. Contact IBM® Software Support if you are unable to resolve the error.
Parent topic: Error messages and codes: AUIYxxxx

AUIY007I Invoking callable service *callable service*.

Explanation

The specified callable service has been invoked successfully.

User response

No action is required.
Parent topic: Error messages and codes: AUIYxxxx

AUIY008I Returned from callable service *service-name*

Explanation

Returned from a callable service that is identified in the message.

User response

No action is required.

Parent topic: Error messages and codes: AUIYxxxx

AUIY009E Invalid data set mask: *data set mask*.

Explanation

The specified data set mask is not valid.

User response

Enter a valid data set mask and retry.
Parent topic: Error messages and codes: AUIYxxxx

Error messages and codes: AUIZxxxx

The following information is about error messages and codes that begin with AUIZ.

- **AUIZ002E**
  dd-name DD has already been allocated.
- **AUIZ003W**
  Attached to existing shared memory segment.
- **AUIZ004S**
  Shared memory segment key verification failed ('*key-value*').
- **AUIZ005S**
  Shared memory segment eyecatcher 'value' invalid.
- **AUIZ007S**
  The master address space failed to respond to a connect request.
- **AUIZ008W**
  IBM® Security Guardium® S-TAP® for IMS on z/OS® agent failed to shut down properly last time.
- **AUIZ009S**
  Attempts to attach to shared memory segment *segment key* failed.
- **AUIZ010W**
  Configuration value for <*parameter*> is set below the allowed minimum of <*limit*>.
- **AUIZ011W**
  Configuration value for <*parameter*> is set above the allowed maximum of <*limit*>.

- **AUIZ012I**
  Log-server: listening on port *<port>*.
- **AUIZ013E**
  Log-server: no available port was found in the range *<min-port>-<max-port>*.
- **AUIZ014W**
  Log-server: invalid data received from client *<client-ip>* (*<header-data>*).
- **AUIZ020W**
  Configuration parameter *parameter-name* was ignored: duplicate value specified *specified-value*.
- **AUIZ021E**
  Configuration parameter *option* can't be empty.
- **AUIZ022E**
  At least one active appliance is required.
- **AUIZ023E**
  Duplicate appliance specified: *host/port*.
- **AUIZ024E**
  Duplicate appliance priority specified: *priority*.
- **AUIZ025E**
  Spill size can't be zero if more than one appliance is enabled.
- **AUIZ026E**
  Configuration parameter *<option>* value *<value>* is invalid; expected list *<value-list>*.
- **AUIZ027W**
  Host name can't be resolved *<host-name>*.
- **AUIZ028E**
  Configuration parameter *element-name* value *element-value* is invalid: expected min *value-min* and max *value-max*.
- **AUIZ029E**
  Property *property-name* not found in config.
- **AUIZ030E**
  Configuration parameter *parameter-name* value *parameter-value* is not valid long value.
- **AUIZ031E**
  Configuration parameter *parameter-name* value *parameter-value* is not valid unsigned long value.
- **AUIZ032E**
  Configuration parameter *parameter-name* value *parameter-value* is not valid short value.
- **AUIZ033E**
  Configuration parameter *parameter-name* value *parameter-value* is not valid unsigned short value.
- **AUIZ034E**
  Configuration parameter *parameter-name* value *parameter-value* is not valid boolean value.
- **AUIZ035E**
  Configuration parameter *parameter-name* value *parameter-value* is not valid double value.
- **AUIZ036E**
  Configuration parameter *element-name* value *element-value* length is invalid: expected min *length-min* and max *length-max* characters.
- **AUIZ037I**
  Collection profile *profile* uninstalled successfully.
- **AUIZ038I**
  Collection profile *profile* installed successfully.
- **AUIZ039I**
  Guardium policy processing started.
- **AUIZ040I**
  Guardium policy processing finished [active = *<number1>*, installed = *<number2>*, uninstalled = *<number3>*].
- **AUIZ041E**
  Profile for IMS source *ims_name* was ignored: unknown IMS.
- **AUIZ041W**
  Profile for IMS source *ims_name* was ignored: unknown IMS.
- **AUIZ042W**
  IMS artifact *ims-name* was ignored: invalid IMS definition.
- **AUIZ043E**
  XCF callable service invocation failed: function *function-name*, RC = *nn*, reason code = *hhhhhhhh*, AUIU proc name = *proc-name*, ADS_SHR_MEM ID = *nn*.
- **AUIZ044S**
  Shared memory segment version *S-TAP version found* is not compatible with expected *expected version*.
- **AUIZ045E**
  AUICONFG DD must be allocated.
- **AUIZ046E**
  module-name callable service invocation failed: RC = *return-code*, reason code = *reason-code*.
- **AUIZ047E**
  Specified spill file *data_set_name* does not exist.
- **AUIZ048E**
  Problem encountered for *<spill>*, *<problem area>*: required *<req>*, received *<res>*.
- **AUIZ049E**
  z/OS call failure for *<spill>*, *<problemarea>*: RC= *<rc>*, RSN= *<rsn>*.
- **AUIZ050E**
  Specified Log Stream 'xxx.xxx.xxx' does not exist
- **AUIZ051E**
  Problem encountered while validating *log-stream-name*. Function: *request: CONNECT*, RC = *xx*, RSN = *zzzz*.
- **AUIZ052E**
  Abend occurred while validating *<log stream>*. Abend code = *<code>*, RSN=*<reason>*.
- **AUIZ053E**
  Logging subsystem failed to initialize successfully.
- **AUIZ054E**
  The Batch DLI log Stream and Online DLI log stream names must be different.
- **AUIZ055E**
  Shared memory segment ID *<shm-id>* is not available for use.

- **AUIZ056E**
  Shared memory segment ID *segment_id* is owned by agent *agent_name* and cannot be attached.
- **AUIZ057E**
  A configuration syntax error was detected at line *<number>*; expected "*<token1>*", found "*<token2>*".
- **AUIZ058I**
  Collection profile *<profile-name>* updated successfully.
- **AUIZ059E**
  Configuration parameter *<option>* value *<value>* is invalid: the first character must be alphabetic.
- **AUIZ060E**
  The master address space did not respond within 60 seconds.
- **AUIZ061I**
  AUIHOST file has been detected.
- **AUIZ062I**
  AUIHOST file LPAR name/DNS name overrides in use: CVTS_LPAR_NAME(DNS_NAME)
- **AUIZ063E**
  AUIHOST file format is invalid. RECFM must be FB; LRECL must be 80.
- **AUIZ064E**
  AUIHOST file contains invalid syntax *<line number and string>*
- **AUIZ065W**
  IMS STAP *<name>* TCP/IP streaming disabled due to user settings.
- **AUIZ066E**
  Configuration parameter "DLIFREQ" value *value* is invalid: expected 10K-999K, 1M-10M.
- **AUIZ067W**
  Configuration parameter *<parameter>* value *<wrong value>* is not valid. *<Value>* will be used instead.

Parent topic: Messages and codes for IBM Security Guardium S-TAP for IMS on z/OS

AUIZ002E *dd-name* DD has already been allocated.

Explanation

The *dd-name* DD needed for the task, has been previously allocated.

System action

The task terminates with a return code of 12.

User response

dd-name DD is dynamically allocated. Ensure that the *dd-name* DD is not present in the task JCL. If the *dd-name* is not present in the JCL, contact IBM® Software Support.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ003W Attached to existing shared memory segment.

Explanation

This message corresponds to message AUIZ008W. This message indicates that the memory segment has been cleaned, and is being reused.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ004S Shared memory segment key verification failed ('*key-value*').

Explanation

Shared memory segment validation failed. This usually implies that the shared memory segment is owned by another product or system.

User response

Change shared memory segment id and restart the agent:

```
ADS_SHR_MEM_ID
```

Parent topic: Error messages and codes: AUIZxxxx

AUIZ005S Shared memory segment eyecatcher 'value' invalid.

Explanation

Shared memory segment validation failed. This implies that the shared memory segment is owned by another product or system.

User response

Change shared memory segment ID and restart the agent:

`ADS_SHR_MEM_ID`

Parent topic: Error messages and codes: AUIZxxxx

AUIZ007S The master address space failed to respond to a connect request.

Explanation

A secondary address space failed to connect to the master address space.

User response

Check the listener-port in the address-space-manager-config section of the configuration and verify that it matches in both AUICONFG and members of the primary address space and secondary address spaces.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ008W IBM® Security Guardium® S-TAP® for IMS on z/OS® agent failed to shut down properly last time.

Explanation

When the agent is restarting, the persistent memory object indicates that the agent was abnormally cancelled or terminated without going through the proper clean-up routines, for example, Estae processing. This message might also indicate that another instance of the agent is currently executing.

User response

Verify that there is only one instance of this agent running.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ009S Attempts to attach to shared memory segment *segment key* failed.

Explanation

This error message always occurs in conjunction with error message AUIX013E.

This startup error indicates that attempts to create a shared memory segment failed because of an already existing shared memory segment that never belonged to, or currently does not belong to, the primary agent address space.

This message can occur in the secondary address space if the <id> elements in the <address-space-manager-config> parameters of the AUICONFG config member that is used by the agent primary address space and the secondary address spaces(s) do not match.

User response

Edit SAUISAMP member AUICONFG (or the customized AUICONFG) and specify a different <id> element in the <address-space-manager-config> section.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ010W Configuration value for *<parameter>* is set below the allowed minimum of *<limit>*.

Explanation

Configuration parameter is not valid: *<parameter>* should be not less than *<limit>*.

User response

Change the parameter to comply with the requirements.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ011W Configuration value for *<parameter>* is set above the allowed maximum of *<limit>*.

Explanation

Configuration parameter is not valid: <parameter> should exceed the *<limit>*.

User response

Change the parameter to correspond to the requirements.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ012I Log-server: listening on port *<port>*.

Explanation

Identifies the port number that the Log-server is listening to.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ013E Log-server: no available port was found in the range *<min-port>-<max-port>*.

Explanation

No available port was found in specified range. This usually implies that the range of ports is used by other installations or products.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ014W Log-server: invalid data received from client *<client-ip>* (*<header-data>*).

Explanation

This message indicates that an unexpected connection occurred from *<client-ip>* to log-server port.

System action

The connection is refused, and processing continues.

User response

This warning message can be produced during a system-level port security scan. If you do not want to receive this message, suppress it by using the configuration parameters LOG_FILTER(E) and LOG_FILTER_MSGS_ID(AUIZ014W).

If a port scan was not active when this message was received, it indicates that an unknown message was received by the log-server port. Contact IBM Software Support.

Parent topic: Error messages and codes: AUIZxxxx

AUIZ020W Configuration parameter *parameter-name* was ignored: duplicate value specified *specified-value*.

Explanation

The specified configuration parameter *parameter-name* cannot contain a value that has already been specified for a related parameter.

User response

Fix the duplicate value *specified-value* and restart the agent.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ021E Configuration parameter *option* can't be empty.

Explanation

The configuration parameter *option* contains an invalid value.

User response

Check the valid values for the *option* and correct the configuration file.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ022E At least one active appliance is required.

Explanation

No appliances were specified in the agent configuration, or all specified appliances were disabled.

User response

Check agent configuration and add enabled appliances to configuration.

Parent topic: Error messages and codes: AUIZxxxx

AUIZ023E Duplicate appliance specified: *host/port*.

Explanation

Specified appliance (*host/port*) are duplicates of another appliance specified in the configuration.

User response

Update or remove duplicate appliances in the agent configuration.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ024E Duplicate appliance priority specified: *priority*.

Explanation

Two or more appliances with duplicate priority (*priority*) were specified.

User response

Update or remove appliances with duplicate priorities in the agent configuration.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ025E Spill size can't be zero if more than one appliance is enabled.

Explanation

Spill size should be greater than zero if two or more active appliances are specified.

User response

Specify a valid spill size.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ026E Configuration parameter *<option>* value *<value>* is invalid; expected list *<value-list>*.

Explanation

The configuration parameter *<option>* contains an invalid value.

User response

Check the valid values for the *<option>* and correct the configuration file.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ027W Host name can't be resolved *<host-name>*.

Explanation

An attempt was made to determine the IP address of the host name that was indicated through the use of the z/OS *getaddrinfo* service. The attempt failed.

System action

If the host name is not the local LPAR, processing continues. The TCP/IP address for any events that occur on this LPAR will not be sent to the appliance for reporting. If the host name is the local LPAR where the agent (AUIAstc task) is running, the local host name and IP address will be used for INTER and INTRA task communications.

User response

The z/OS network administrator must verify that the LPAR name exists in the DNS table.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ028E Configuration parameter *element-name* value *element-value* is invalid: expected min *value-min* and max *value-max*.

Explanation

The *element-value* given for *element-name* is out of the range and must be within *min-value* and *max-value*.

User response

Correct the value for the *element-name* in the configuration.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ029E Property *property-name* not found in config.

Explanation

A required property *property-name* could not be loaded from the configuration file because it has been incorrectly specified, specified multiple times, or not specified at all.

User response

Update configuration file and add *property-name* with an appropriate value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ030E Configuration parameter *parameter-name* value *parameter-value* is not valid long value.

Explanation

The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *long*.

User response

Correct the configuration value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ031E Configuration parameter *parameter-name* value *parameter-value* is not valid unsigned long value.

Explanation

The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *unsigned long*.

User response

Correct the configuration value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ032E Configuration parameter *parameter-name* value *parameter-value* is not valid short value.

Explanation

The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *short*.

User response

Correct the configuration value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ033E Configuration parameter *parameter-name* value *parameter-value* is not valid unsigned short value.

Explanation

The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *unsigned short*.

User response

Correct the configuration value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ034E Configuration parameter *parameter-name* value *parameter-value* is not valid boolean value.

Explanation

The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *boolean*.

User response

Correct the configuration value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ035E Configuration parameter *parameter-name* value *parameter-value* is not valid double value.

Explanation

The configuration parameter identified by *parameter-name* contains an invalid value. The expected value should be of type *double*.

User response

Correct the configuration value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ036E Configuration parameter *element-name* value *element-value* length is invalid: expected min *length-min* and max *length-max* characters.

Explanation

The *element-value* given for *element-name* is too long and its length must be within *length-min* and *length-max*.

User response

Correct the value for the *element-name* in the configuration file.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ037I Collection profile *profile* uninstalled successfully.

Explanation

The specified collection profile uninstalled.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ038I Collection profile *profile* installed successfully.

Explanation

The specified collection profile installed.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ039I Guardium® policy processing started.

Explanation

The agent has received a policy message from the appliance and has started to process it.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ040I Guardium® policy processing finished [active = *<number1>*, installed = *<number2>*, uninstalled = *<number3>*].

Explanation

The Guardium policy has been processed. The active, installed, and uninstalled values indicate the number of processed collection profiles.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ041E Profile for IMS source *ims_name* was ignored: unknown IMS.

Explanation

The agent received an IMS policy from the Security Guardium® system which does not relate to this agent instance.

System action

The policy is ignored by this agent.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ041W Profile for IMS source *ims_name* was ignored: unknown IMS.

Explanation

The agent received an IMS policy from the Security Guardium® system which does not relate to this agent instance.

System action

The policy is ignored by this agent.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ042W IMS artifact *ims-name* was ignored: invalid IMS definition.

Explanation

During policy pushdown, an *ims-name* was specified for one of the rules that does not exist in the Guardium® appliance.

User response

Contact IBM® Software Support.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ043E XCF callable service invocation failed: function *function-name*, RC = *nn*, reason code = *hhhhhhhh*, AUIU proc name = *proc-name*, ADS_SHR_MEM ID = *nn*.

Explanation

An error occurred attempting to retrieve AUIU tokens from the CF.

User response

If the LPAR is not a sysplex member, no action is necessary. If the LPAR is a sysplex member, please contact IBM® Software Support.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ044S Shared memory segment version *S-TAP version found* is not compatible with expected *expected version*.

Explanation

An attempt to attach to a shared memory segment failed because of version mismatch. This might indicate that the shared memory segment that is identified by ADS_SHR_MEM_ID is already in use by an older version of the product, or another product.

User response

Verify and change the ADS_SHR_MEM_ID that is specified in the agent configuration.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ045E AUICONFG DD must be allocated.

Explanation

The address space requires an AUICONFG DD to be specified in the JCL.

User response

Update the JCL for the address space to include an AUICONFG DD.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ046E *module-name* callable service invocation failed: RC = *return-code*, reason code = *reason-code*.

Explanation

Invocation of the specified module failed due to the specified *return-code* and *reason-code*.

User response

Contact IBM Software Support.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ047E Specified spill file *data_set_name* does not exist.

Explanation

During agent startup, the SMF spill file that is named in the configuration parameter SMF_SPILL_FILE(dsn) was not found.

System action

The agent terminates.

User response

Determine why the file cannot be located. Correct any errors, and restart the agent.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ048E Problem encountered for *<spill>*, *<problem area>*: required *<req>*, received *<res>*.

Explanation

This spill data set *<spill>* could not be validated. The *<problem area>* with the parameters *<req>* and *<res>* gives additional details.

User response

Fix the issue in the *<problem area>* using the required *<req>* value. If necessary, contact IBM® Software Support for additional help.

Parent topic: Error messages and codes: AUIZxxxx

AUIZ049E z/OS call failure for *<spill>*, *<problemarea>*: RC= *<rc>*, RSN= *<rsn>*.

Explanation

An attempt to validate the spill data set has caused an error with the z/OS services. A *<problemarea>* value with return code *<rc>* and reason code *<rsn>* are returned. If the *<problemarea>* value is *OBTAIN*, and the *<rc>* value is 4, the spill database in question might have been migrated. In that case, the spill database should be recalled before processing continues.

User response

If a migrated data set is not the problem, contact IBM Software Support.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ050E Specified Log Stream 'xxx.xxx.xxx' does not exist

Explanation

The z/OS log stream name that was specified in the LOG_STREAM_DLIO or LOG_STREAM_DLIB AUICONFG DD input stream does not exist.

System action

The agent address space terminates.

User response

Correct the log stream name that you provided, or customize and run the AUILSTRx Log Stream definition jobs that are located in the SAUISAMP product data set.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ051E Problem encountered while validating *log-stream-name*. Function: *request: CONNECT*, RC = *xx*, RSN = *zzzz*.

Explanation

There was a failed attempt to validate the z/OS® System Logger Log-Stream, through the use of an IXGCONN call.

System action

Processing terminates.

User response

Determine the cause of the failure by examining the return and reason codes for the IXGCONN macro. These can be found in the manual, *IBM® MVS™ Programming: Authorized Assembler Services References*.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ052E Abend occurred while validating *<log stream>*. Abend code = *<code>*, RSN= *<reason>*.

Explanation

The Log Stream *<log stream>* validation failed with abend code *<code>* and reason code *<reason>*.

User response

Contact IBM® Software Support.

Parent topic: Error messages and codes: AUIZxxxx

AUIZ053E Logging subsystem failed to initialize successfully.

Explanation

This error can occur for several reasons. It is preceded by the specific occurrence that caused the logging subsystem to fail during initialization.

User response

Review previously issued error messages to determine the cause of the logging failure.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ054E The Batch DLI log Stream and Online DLI log stream names must be different.

Explanation

The log stream name specified for LOG_STREAM_DLIO and LOG_STREAM_DLIB must be different.

User response

Specify different log streams for batch and online in the agent configuration.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ055E Shared memory segment ID *<shm-id>* is not available for use.

Explanation

The shared memory segment ID *<shm-id>* that is specified in the configuration file is not available, or is used by another task.

User response

Check the available *<shm-id>* and update the confugration files. Contact IBM® Software Support if *<shm-id>* is set correctly.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ056E Shared memory segment ID *segment_id* is owned by agent *agent_name* and cannot be attached.

Explanation

The shared memory segment that was identified by the <id> parameter within the address-space-manager-config section of the agent configuration file is already used by the specified agent, *agent_name*.

System action

The agent terminates because it is unable to use the shared memory segment.

User response

To avoid a collision with other agents running on the LPAR, change or include the <id> value in the address-space-manager_config section of the agent configuration file.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ057E A configuration syntax error was detected at line *<number>*; expected "*<token1>*", found "*<token2>*".

Explanation

An invalid value was found in the AUICONFG file and the indicated line.

System action

Processing terminates.

User response

Review Configuring the IBM Security Guardium S-TAP for IMS on z/OS agent for information about permissible configuration values. Correct the syntax error and restart the agent.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ058I Collection profile *<profile-name>* updated successfully.

Explanation

The active collection profile *<profile-name>* has been updated during policy installation.

User response

No action is required.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ059E Configuration parameter *<option>* value *<value>* is invalid: the first character must be alphabetic.

Explanation

The configuration parameter *<option>* contains an invalid value.

User response

Review the valid values for the *<option>* and correct the configuration file.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ060E The master address space did not respond within 60 seconds.

Explanation

The IBM® Guardium® S-TAP® for IMS agent did not send the policy report to the Memory Management Utility (AUIU*STC*) task within 60 seconds of establishing the connection.

System action

The AUIU*STC* task terminates with RC=12.

User response

Contact IBM Software Support.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ061I AUIHOST file has been detected.

Explanation

The AUIHOST DD statement has been detected in the JCL.

System action

The IP address for participating LPARs are resolved by the information contained in this file and described by message AUIxxxI.

User response

If this was not intended, remove the DD statement.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ062I AUIHOST file LPAR name/DNS name overrides in use: CVTS_LPAR_NAME(DNS_NAME)

Explanation

The AUIHOST DD has provided an override for the host named.

System action

The DNS_NAME is the value that is used to perform the gethostbyname call in order to obtain the relevant IP address.

User response

Verify that the supplied LPAR_NAME and DNS_NAME values are correct.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ063E AUIHOST file format is invalid. RECFM must be FB; LRECL must be 80.

Explanation

The file format that was provided by using the AUIHOST DD is incorrect.

System action

The address space terminates.

User response

Verify that the supplied file is a Fixed Block (FB) sequential file, has a logical record length (LRECL) of 80 bytes, and is a either a sequential file or a member of a Partitioned Data Set (PDS or PDS/E). Correct the error and restart the address space.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ064E AUIHOST file contains invalid syntax *<line number and string>*

Explanation

The AUIHOST file supplied contains a record with invalid syntax.

System action

The address space terminates.

User response

Review the Overriding the TCP/IP DNS resolver table topic to verify the required syntax. Correct the record and restart the address space.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ065W IMS STAP <*name*> TCP/IP streaming disabled due to user settings.

Explanation

Simulation mode is on because the STAP_STREAM_EVENTS parameter has been set to N.

System action

Events will not be streamed to the Guardium® system.

User response

To stream events to the Guardium system, set the STAP_STREAM_EVENTS parameter to Y.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ066E Configuration parameter "DLIFREQ" value *value* is invalid: expected 10K-999K, 1M-10M.

Explanation

In the AUICONFG file, the DLIFREQ parameter value is outside of the permitted range. Valid values for the DLIFREQ parameter are 10K -- 999K, or 1M -- 10M.

System action

The AUIA*xxx* task terminates.

User response

Correct the DLIFREQ parameter value.
Parent topic: Error messages and codes: AUIZxxxx

AUIZ067W Configuration parameter <*parameter*> value <*wrong value*> is not valid. <*Value*> will be used instead.

Explanation

Configuration parameter is not valid: <*parameter*> should match <*value*>.

User response

Change the parameter to correspond to the requirements.
Parent topic: Error messages and codes: AUIZxxxx

IBM Security Guardium S-TAP for Data Sets on z/OS

These topics describe how to use IBM Security Guardium S-TAP for Data Sets on z/OS V10.1.3 (also referred to as IBM Guardium S-TAP for Data Sets). The V10.1.3 S-TAP is optimized for the V10.1 Guardium system. IBM Guardium S-TAP for Data Sets collects and correlates data access information from a variety of resources to produce a comprehensive view of business activity for auditors.

About these topics

This information is designed to help database administrators, system programmers, and application programmers perform these tasks:

- Plan for the installation of IBM Guardium S-TAP for Data Sets
- Install and operate IBM Guardium S-TAP for Data Sets
- Configure the IBM Guardium S-TAP for Data Sets environment
- Diagnose and recover from IBM Guardium S-TAP for Data Sets problems

A PDF of this User's Guide is also available here.

- **IBM Security Guardium S-TAP for Data Sets on z/OS overview**
  IBM Security Guardium S-TAP for Data Sets on z/OS (also referred to as IBM Guardium S-TAP for Data Sets) collects and correlates data access information from System Management Facilities (SMF) records and realtime system events to produce a comprehensive view of data set access activity for auditors.
- **Installation requirements for IBM Guardium S-TAP for Data Sets V10.1.3**
  Review the software and authorization prerequisites for installing IBM Guardium S-TAP for Data Sets V10.1.3.
- **Configuring the IBM Guardium S-TAP for Data Sets agent**
  You must configure the IBM Guardium S-TAP for Data Sets agent.
- **IBM Guardium S-TAP for Data Sets administration**
  You must configure the Guardium system to communicate with the IBM Guardium S-TAP for Data Sets agent.
- **Reference information**
  This section provides IBM Guardium S-TAP for Data Sets reference information.
- **Troubleshooting**
  Use these topics to diagnose and correct problems that you might experience with IBM Guardium S-TAP for Data Sets.

Parent topic: S-TAP for z/OS V10.1.3 User's Guide

IBM Security Guardium S-TAP for Data Sets on z/OS overview

IBM Security Guardium S-TAP for Data Sets on z/OS (also referred to as IBM Guardium S-TAP for Data Sets) collects and correlates data access information from System Management Facilities (SMF) records and realtime system events to produce a comprehensive view of data set access activity for auditors.

IBM Guardium S-TAP for Data Sets enables you to collect many different types of information, including:

- Access to VSAM and non-VSAM data sets and security violations that are recorded by SMF.
- Data set operations that are performed against VSAM data sets, such as delete or rename events, recorded by SMF.
- Access to specific records within VSAM data sets, including key-sequenced data sets (KSDS) or relative record data sets (RRDS), captured as they occur.
- Transaction information that is associated with a VSAM KSDS or RRDS logical record operation, performed within a transaction that runs on the Customer Information Control System (CICS) Transaction Server.
- Access to read and update events for a particular VSAM cluster (consisting of one or more physical data sets) for actions performed on the data set as a whole, or actions performed at the individual level for records within the data set.

- **What's new in IBM Guardium S-TAP for Data Sets V10.1.3?**
  Speed and monitoring enhancements are now provided in V10.1.3.
- **IBM Guardium S-TAP for Data Sets components**
  IBM Guardium S-TAP for Data Sets consists of its data collection agent and the Security Guardium system. The IBM Guardium S-TAP for Data Sets agent collects data set access information that is obtained from the SMF record exit interface, as well as record access information that is obtained from individual I/O requests. The Guardium system is a server-based component that provides the product user interface.

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS

What's new in IBM Guardium S-TAP for Data Sets V10.1.3?

Speed and monitoring enhancements are now provided in V10.1.3.

Enhanced reporting of partitioned data sets (PDS) and extended partitioned data sets (PDSE) member activity
: IBM Guardium S-TAP for Data Sets can now report on the following types of activity:

  - Member Adds
  - Member Replaces
  - Member Renames
  - Member Deletes
  - STOW Initialization (PDSE directory clearing)

New Simulation option
: Enabling Simulation mode enables you to assess the impact of data collection processing without streaming data to the Guardium appliance.

Increased CICS transaction server support
: IBM Guardium S-TAP for Data Sets supports collection of:

  - CICS Transaction Server 5.3 to capture Record Level Monitoring (RLM) data
  - 8-character CICS local unit of work (with CICS Transaction Server 4.2 and later, until end of service)
  - Dynamic starting and stopping of RLM data collection with new IBM Guardium S-TAP for Data Sets SAMPLIB members

Ability to restrict reporting of sensitive data
: When enabled, the FORCE_LOG_LIMITED parameter enables you to restrict Personally Identifiable Identification (PII) from being sent to the Guardium system.

Reporting of FTP activity
: In addition to monitoring of JES2, JES3, ASCH, TSO, and STC address spaces, IBM Guardium S-TAP for Data Sets provides OMVS address space monitoring. This enables reporting of FTP activity.

Reporting of FTP transmission of non-VSAM data sets
: IBM Guardium S-TAP for Data Sets enables you to audit FTP transmission of non-VSAM data sets to and from monitored systems.

New filtering criteria for data set accesses
: For VSAM and non-VSAM Data Sets Close events, you can filter by input-only, output-only, or both input and output events.

Support for Internet Protocol version 6 (IPV6)
: PH16991 introduces IPV6 support and new subsystem configuration option, PREFER_IPV4_STACK.

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS overview

IBM Guardium S-TAP for Data Sets components

IBM Guardium S-TAP for Data Sets consists of its data collection agent and the Security Guardium system. The IBM Guardium S-TAP for Data Sets agent collects data set access information that is obtained from the SMF record exit interface, as well as record access information that is obtained from individual I/O requests. The Guardium system is a server-based component that provides the product user interface.

Guardium system and S-TAP agent communication

Communication between the Guardium system and the agent uses a TCP/IP connection. The collection policies that you create, by using the Guardium system user interface, tell the agent what types of data to collect. The policies specify filter information, such as which jobs and data sets to monitor for data accesses.

Guardium system

Use the Guardium system to gather and generate reports on information from multiple agents that are running on multiple z/OS® systems. The Guardium system:

- Provides the user interface, which processes your requests and displays the resulting information.
- Enables you to create collection policies, which specify the types of data that are to be collected by the agent.

- Stores the collected data.

Agent

The agent collects data from a single z/OS system. Monitoring can be performed at both the data set and record level:

- For data set level monitoring, data is collected directly from SMF records, as presented to various SMF exits with which the agent interfaces.
- For record level monitoring, data is collected when VSAM records are read or written.

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS overview

Installation requirements for IBM Guardium S-TAP for Data Sets V10.1.3

Review the software and authorization prerequisites for installing IBM Guardium S-TAP for Data Sets V10.1.3.

- **Software prerequisites**
  IBM Guardium S-TAP for Data Sets requires z/OS Version 2 Release 2 or later, until end of service.
- **User ID authority requirements**
  To install the product, you must have the necessary z/OS user ID authorities.

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS

Software prerequisites

IBM Guardium S-TAP for Data Sets requires z/OS® Version 2 Release 2 or later, until end of service.

Customer Information Control System (CICS®) Transaction Server support requires IBM CICS Transaction Server for z/OS V4 Release 2 or later, until end of service.

Parent topic: Installation requirements for IBM Guardium S-TAP for Data Sets V10.1.3

User ID authority requirements

To install the product, you must have the necessary z/OS® user ID authorities.

Your z/OS user ID must have the authority to:

- Define the appropriate SMF record collection parameters in the SMFPRMxx PARMLIB member and APF authorize the load library for the product.
- Update the appropriate procedure library to include the agent started task.

If you choose to enable CICS support, you must also have the authority to:

- Update CICS parameters.
- Add CICS program definitions.
- Update or create CICS system initialization and termination program list tables for startup and shutdown.

If necessary, contact your system administrator to obtain the required authorities.
Parent topic: Installation requirements for IBM Guardium S-TAP for Data Sets V10.1.3

Configuring the IBM Guardium S-TAP for Data Sets agent

You must configure the IBM Guardium S-TAP for Data Sets agent.

Configuration overview

To configure the product, complete the required steps.

- Security: Review and establish the security requirements. You must set up access controls in your security product in order to create, authorize, or update the various data sets that are necessary for product configuration.
- Review the required resource authorizations information, including:
  - APF authorizing the load library
  - Authorizing the z/OS agent started task for the control data set
  - Defining an OMVS segment
- Planning your configuration: Review the steps that are required to plan your configuration.
  - Job cards for the sample JCL in the sample library: Provide valid job cards.
  - Allocating auxiliary storage: Ensure that data will not be lost in the event of an overflow.
- Configuring the SMFPRMxx parameter library member: Ensure a complete audit by configuring the SMFPRMxx parameter library to collect the required SMF record types.
- IAM and ACF2 collection considerations: Review information about capturing IAM data set activity and ACF2 access failures.
- Creating the control data set: Generate the initial partitioned data set members.
- Specifying subsystem options: Review the subsystem changes that you can make to the options member in the control data set.
- Configuring the started task JCL: Determine the location of the started task control job language (JCL), and follow configuration steps and tips.
- CICS Transaction Server support: Review the requirements for enabling the CICS Transaction Server, and follow the instructions for Configuring CICS Transaction Server support.

- **Security**
  IBM Guardium S-TAP for Data Sets requires access to various z/OS data sets and system components. You must set up access controls in your security product in order to create, authorize, or update the various data sets that are necessary for product configuration.

- **Planning your configuration**
  Use this planning list to determine necessary information before continuing. Then, provide a valid job card, and allocate auxiliary storage if necessary, as described in the following sections.
- **Configuring the SMFPRMxx parameter library member**
  To ensure a complete audit, you must configure the active SMFPRMxx member of the z/OS system PARMLIB to collect the required SMF record types needed by IBM Guardium S-TAP for Data Sets.
- **IAM and ACF2 collection considerations**
  IBM Guardium S-TAP for Data Sets can capture IAM data set activity and ACF2 access failures. Learn how to enable IBM Guardium S-TAP for Data Sets to collect this information, and be aware of the following collection considerations. These products implement the collection of SMF data in a nonstandard way and require special consideration.
- **Creating the control data set**
  Complete these steps to create the control data set and generate the initial partitioned data set (PDS) members. These members contain required information, and must be added to the newly created data set for the agent to work correctly.
- **Specifying subsystem options**
  To configure IBM Guardium S-TAP for Data Sets, you must specify a four-character IBM Guardium S-TAP for Data Sets subsystem ID (SUBSYS) to associate with this particular instance of IBM Guardium S-TAP for Data Sets. The SUBSYS identifies the IBM Guardium S-TAP for Data Sets subsystem in messages that are generated by the product.
- **Configuring the started task JCL**
  You must configure the started task JCL statements with values that provide the system with information that is specific to your environment. Follow these steps to configure the started task JCL.
- **CICS Transaction Server support**
  IBM Guardium S-TAP for Data Sets CICS Transaction Server support enables you to filter and capture CICS transaction information.
- **Configuring CICS signon reporting**
  IBM Guardium S-TAP for Data Sets can identify the CICS signon that was used for a specific file access event. Configure the product to enable the agent to send the CICS signon information to the Guardium system.
- **Starting the product**
  Start IBM Guardium S-TAP for Data Sets before starting products that perform similar functions.
- **Sample library members**
  The following sample library members are included for your use in installing and configuring IBM Guardium S-TAP for Data Sets. The following table lists them by type and description.
- **Verifying the installation**
  After you install and configure the IBM Guardium S-TAP for Data Sets agent, verify that the agent is properly installed. Use the JCL that is provided in the AUVJIVP member of the SAUVSAMP sample library.

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS

Security

IBM Guardium S-TAP for Data Sets requires access to various z/OS® data sets and system components. You must set up access controls in your security product in order to create, authorize, or update the various data sets that are necessary for product configuration.

To provide IBM Guardium S-TAP for Data Sets with access to the necessary z/OS data sets and system components, you must APF authorize the load library, authorize the z/OS started task for the control data set, and define an OMVS segment to your security product, as described in the following sections.

Security products can include various software tools that are currently available, such as IBM Resource Access Control Facility (RACF®), Computer Associates International Top Secret, and Computer Associates International Access Control Facility (ACF2).

- **APF authorizing the load library**
  IBM Guardium S-TAP for Data Sets requires certain data sets to be accessible and APF authorized on the system on which the agent started task will run. SMF data will be collected by the agent.
- **Authorizing the z/OS agent started task for the control data set**
  The z/OS agent started task must be authorized to read and update the control data set. The control data set is a partitioned data set that contains various members that define options and operating parameters for the product. IBM Guardium S-TAP for Data Sets uses a control data set that is defined in the agent started task.
- **Defining an OMVS segment**
  You must define an OMVS segment to your security product to make use of TCP/IP connectivity and UNIX System Services. An OMVS segment specifies the user ID to be used, the home directory, and the shell program name.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

APF authorizing the load library

IBM Guardium S-TAP for Data Sets requires certain data sets to be accessible and APF authorized on the system on which the agent started task will run. SMF data will be collected by the agent.

The product data set SAUVLOAD, which contains the product load modules that are required for operation, must be APF authorized on the system on which IBM Guardium S-TAP for Data Sets will be run.

Refer to the z/OS MVS Programming Authorized Assembler Services Guide for guidelines and instructions for using APF.

Parent topic: Security

Authorizing the z/OS agent started task for the control data set

The z/OS® agent started task must be authorized to read and update the control data set. The control data set is a partitioned data set that contains various members that define options and operating parameters for the product. IBM Guardium S-TAP for Data Sets uses a control data set that is defined in the agent started task.

Refer to your security product documentation for more information on authorizing the agent started task.

Parent topic: Security

Defining an OMVS segment

You must define an OMVS segment to your security product to make use of TCP/IP connectivity and UNIX System Services. An OMVS segment specifies the user ID to be used, the home directory, and the shell program name.

If you are using IBM RACF, refer to z/OS UNIX System Services Planning for guidelines and instructions about OMVS segment definitions. If you are using a security product other than RACF, refer to your product's instructions on how to define an OMVS segment.

Parent topic: Security

Planning your configuration

Use this planning list to determine necessary information before continuing. Then, provide a valid job card, and allocate auxiliary storage if necessary, as described in the following sections.

Before configuration, you must determine:

- The user who will configure the product
- The user ID that will be used to run the agent
- Where the Guardium system and the S-TAP agent will run

- **Job cards for the sample JCL in the sample library**
  Some JCL members that are included with the product sample library, SAUVSAMP, have a sample card for the job card. Provide a valid job card that conforms to the JCL standards of your site before submitting any of the JCL members.
- **Allocating auxiliary storage**
  z/OS auxiliary storage consists of DASD space that is allocated to the local page data sets. It is used as temporary backup storage for programs and data located in virtual and physical memory. IBM Guardium S-TAP for Data Sets can allocate auxiliary storage space if the OUTAGE_SPILLAREA_SIZE parameter is set in accordance with the following requirements.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Job cards for the sample JCL in the sample library

Some JCL members that are included with the product sample library, SAUVSAMP, have a sample card for the job card. Provide a valid job card that conforms to the JCL standards of your site before submitting any of the JCL members.

Parent topic: Planning your configuration

Allocating auxiliary storage

z/OS auxiliary storage consists of DASD space that is allocated to the local page data sets. It is used as temporary backup storage for programs and data located in virtual and physical memory. IBM Guardium S-TAP for Data Sets can allocate auxiliary storage space if the OUTAGE_SPILLAREA_SIZE parameter is set in accordance with the following requirements.

- The OUTAGE_SPILLAREA_SIZE parameter option instructs the address space to allocate a data space equal in size to the value that you set for OUTAGE_SPILLAREA_SIZE.
- Verify that the current local page space can accommodate a new data space.

Example

Specifying OUTAGE_SPILLAREA_SIZE=64 instructs the address space to allocate 64 MB of data space.

Refer to the z/OS® MVS™ Initialization and Tuning guide for more information about sizing local page data sets.
Parent topic: Planning your configuration

Configuring the SMFPRMxx parameter library member

To ensure a complete audit, you must configure the active SMFPRMxx member of the z/OS® system PARMLIB to collect the required SMF record types needed by IBM Guardium S-TAP for Data Sets.

The record types can be collected at the subsystem or system level. Maximum auditing of VSAM and non-VSAM data set activity can be achieved by ensuring that all defined subsystems record all of the SMF record types that are required by the product.

The defaults used at the system level for those subsystems that are not explicitly defined should also specify collection of the required SMF record types. The required SMF record types are 14, 15, 17, 18, 30, 42, 60, 61, 62, 64, 65, 66, and 80. If any required SMF record types are not defined for collection, message AUV1450W alerts you to define them.

If the appropriate exit is not defined for the operating system level, SMF records will not be collected. Specify the SMF exits as follows:

- For z/OS Version 2 Release 2 and earlier, specify the IEFU83, IEFU84, and IEFU85 SMF exits.
- For z/OS Version 2 Release 3 and later, specify the IEFU86 SMF exit.

These exits can be defined at either the subsystem or system level in a manner consistent with the SMF record type specifications.

For more information about setting up and managing SMF, refer to the z/OS MVS™ System Management Facility (SMF) manual.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Related reference

- SMF record types and contexts

IAM and ACF2 collection considerations

IBM Guardium S-TAP for Data Sets can capture IAM data set activity and ACF2 access failures. Learn how to enable IBM Guardium S-TAP for Data Sets to collect this information, and be aware of the following collection considerations. These products implement the collection of SMF data in a nonstandard way and require special consideration.

Innovation Access Method (IAM) from Innovation Data Processing provides capabilities beyond standard VSAM. IAM replaces VSAM access with a proprietary non-VSAM access that simulates VSAM. Because the underlying data sets are non-VSAM, accesses to the IAM-simulated VSAM data sets do not generate VSAM SMF records, such as the SMF type 62 (VSAM OPEN) and SMF type 64 (VSAM CLOSE).

For IAM data sets, IBM Guardium S-TAP for Data Sets does not report the following items:

- Context records for OPEN and UPDATE for IAM data sets (because of the lack of the SMF type 62 records).
- IAM simulation of alternate index and path processing (because of the lack of an IAM SMF CLOSE record).

The CLOSE record counters will report IAM data sets differently from native VSAM processing. Although the IAM CLOSE SMF record offers an extensive array of counters, those corresponding to the VSAM SMF Type 64 record are included in the accumulated counts within the CLOSE context record.

Computer Associates International ACF2 considerations

Unlike some security products, ACF2 does not offer a unique authorization failure code to identify a CONTROL access failure. Instead, it reports these as UPDATE access failures. In ACF2 facilities, no CONTROL context records will be reported.

- **Enabling Innovations Data Processing IAM reporting**
  IAM provides a unique, user-specified record ID, which is written during CLOSE processing. For IBM Guardium S-TAP for Data Sets to report this access:
- **Enabling Computer Associates International ACF2 reporting**
  Access Control Facility (ACF2) from Computer Associates International records access failures to a unique, user-specified record ID. For IBM Guardium S-TAP for Data Sets to report these failures:

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Enabling Innovations Data Processing IAM reporting

IAM provides a unique, user-specified record ID, which is written during CLOSE processing. For IBM Guardium S-TAP for Data Sets to report this access:

Procedure

1. Determine the user-specified SMF record ID that was selected for IAM.
2. Specify that value in the IBM Guardium S-TAP for Data Sets control data set IAM_SMF_RECORD_ID option.

Parent topic: IAM and ACF2 collection considerations

Enabling Computer Associates International ACF2 reporting

Access Control Facility (ACF2) from Computer Associates International records access failures to a unique, user-specified record ID. For IBM Guardium S-TAP for Data Sets to report these failures:

Procedure

1. Determine the user-specified SMF record ID that was selected for ACF2.
2. Specify that value in the IBM Guardium S-TAP for Data Sets control data set ACF_SMF_RECORD_ID option.

Parent topic: IAM and ACF2 collection considerations

Creating the control data set

Complete these steps to create the control data set and generate the initial partitioned data set (PDS) members. These members contain required information, and must be added to the newly created data set for the agent to work correctly.

Before you begin

Refer to the high-level qualifier that you specified when configuring the started task JCL. The same high-level qualifier must be used in step 1 of the control data set creation procedure.

About this task

The options and definitions that determine how IBM Guardium S-TAP for Data Sets performs processing in your environment are contained in the control data set.

Procedure

1. The JCL to create the control data set is located in the AUVJCNTL member of the SAUVSAMP library. Configure the AUVJCNTL member by replacing AUV.V10R1M3 with the high-level qualifier of the installed IBM Guardium S-TAP for Data Sets load library.
2. Submit the JCL to create the control data set.
   The JCL creates the control data set and populates the data set with these initial members: subsystem options (OPTIONS) and policy rule definition members (RULEDEFS and RULEDEFB).
   Important:
   - Do not modify the contents of the RULEDEFS or RULEDEFB member.
   - Do not modify the value of the default INITIAL_RULEDEF option in the RULEDEFS or RULEDEFB members.
3. Specify the APPLIANCE_SERVER and AUDIT parameters in the OPTIONS member to enable the product to function properly.
4. Optional: Consider whether allocating the control data set as an extended partitioned data set (PDSE) is appropriate for your environment.
   A PDSE dynamically manages internal space, drastically reducing the need to perform the space compressions that are required for a nonextended partitioned data set (PDS). The AUVJCNTL member includes statements that can be used to change the allocation to a PDSE.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Specifying subsystem options

To configure IBM Guardium S-TAP for Data Sets, you must specify a four-character IBM Guardium S-TAP for Data Sets subsystem ID (SUBSYS) to associate with this particular instance of IBM Guardium S-TAP for Data Sets. The SUBSYS identifies the IBM Guardium S-TAP for Data Sets subsystem in messages that are generated by the product.

How to use subsystem options

Use either the *keyword=value* or *keyword(value)* format to specify values for these option members.

Option members and descriptions

The IBM Guardium S-TAP for Data Sets subsystem options are in the OPTIONS member of the IBM Guardium S-TAP for Data Sets control data set that is generated by the AUVJCNTL member JCL. These options are the global definitions and general operation options that determine where and how IBM Guardium S-TAP for Data Sets performs its functions.

To specify IBM Guardium S-TAP for Data Sets subsystem options, modify the contents of the OPTIONS member as described.

ACF_SMF_RECORD_ID
: If you are using Access Control Facility (ACF2) from Computer Associates International, you must provide product-specific information for your SMF data to be processed. ACF2 records access failures to a unique record ID. Determine the user-specified SMF record ID that is selected for ACF2 and specify that ID in the IBM Guardium S-TAP for Data Sets CONTROL data set ACF_SMF_RECORD_ID option if you want the product to report these failures.
  ACF2 writes SMF access failure data to a user-defined SMF record ID. Specify a numeric value that identifies the SMF record identification number used by ACF2.
  For ACF2 installations, contact your ACF2 administrator to determine the appropriate numeric value to include with this parameter.
  Note:

  - For z/OS Version 2 Release 3 and later, valid values are 128 – 1151.
  - For z/OS Version 2 Release 2 and earlier, valid values are 128 – 255.

  There is no product default value, however, the SAMPLIB member AUVSOPTS includes a default specification of 230.

APPLIANCE_CONNECT_RETRY_COUNT
: Specify a numeric value that defines the number of times to retry communicating with the Guardium system when an error is encountered during initialization. If the communication is still not successful after the number of retries as specified by this value has been completed, the communication is abandoned and no data is sent. The process also terminates if the number of retries specified is reached with no successful connection.
  Valid values are 0 -- 65535. The default value is 20.

APPLIANCE_NETWORK_REQUEST_TIMEOUT
: Specify a numeric value that defines the number of seconds that must transpire before a timeout is recognized.
  Valid values are 0 -- 65535. The default value, in seconds, is 0.

APPLIANCE_PING_RATE
: Specify a numeric value that defines the number of seconds between pings to the Guardium system. The ping signals the Guardium system that the S-TAP is active and available for communications.
  Valid values are 1 -- 65535. The default value, in seconds, is 5.

APPLIANCE_PORT
: Specify a numeric value that defines the TCP/IP port number for communication with the Guardium system by IBM Guardium S-TAP for Data Sets. Use port 16022 for the V10.1.3 system protocol.
  The default value is 16022.
  If port 16023 is used, encryption support is required for the connection to the appliance.
  Note: Specifying this keyword and parameter designates the port on which the Guardium appliance is listening to the S-TAP. The port is dedicated to the IP address of the appliance. Port 16022 or 16023 can also be in use on z/OS® by another application.
  Valid values are 16022 and 16023.

APPLIANCE_RETRY_INTERVAL
: Specify a numeric value that defines the number of seconds between retries when an error is encountered during an initial attempt to connect to the Guardium system.
  Valid values are 0 -- 65535. The default value, in seconds, is 10.

APPLIANCE_SERVER
: Specify the TCP/IP address for the Guardium system with which IBM Guardium S-TAP for Data Sets is to communicate. In multistream processing scenarios, this address specifies the first Guardium appliance that is to be used.
  The address can be specified as a host name (*security.guardiumvsam.net*) or as four numbers separated by periods (for example, 188.128.6.42).
  Maximum length is 53 characters. There is no default.

APPLIANCE_SERVER_[1-5]
: Specify alternative TCP/IP addresses to use for failover recovery processing and multistream Guardium appliance destinations. Up to five alternative TCP/IP addresses are supported.
  To specify one or more entries, include this parameter with a numeric suffix from 1 - 5. Provide a unique TCP/IP address for each entry.
  The option syntax is as follows:

- APPPLIANCE_SERVER_1=*addr*

or

- APPPLIANCE_SERVER_1(*addr*)

where 1 can be 1, 2, 3, 4, or 5.
Valid values are any valid TCP/IP address. There are no default values. If initialization does not detect this parameter, it does not activate the failover process.
Both the APPLIANCE_SERVER_[1-5] and APPLIANCE _SERVER_FAILOVER_[1-5] parameters can be used to designate servers for multistreaming or failover. Use the APPLIANCE_SERVER_LIST parameter to designate how these parameters are used.
Maximum length is 51 characters.

APPLIANCE_SERVER_FAILOVER_[1-5]

Specify alternative TCP/IP addresses to use for failover and recovery processing. The product supports up to five alternative TCP/IP addresses. To specify one or more entries, include this parameter with a numeric suffix from 1 - 5, each time providing a unique TCP/IP address.
The option syntax is as follows:

```
APPPLIANCE_SERVER_FAILOVER_1=addr
```

or

```
APPPLIANCE_SERVER_FAILOVER_1(addr)
```

where *1* can be 1, 2, 3, 4, or 5.
Valid values are any valid TCP/IP address. There are no default values. If initialization does not detect this parameter, it does not activate the failover process.
Both the APPLIANCE _SERVER_FAILOVER_[1-5] and APPLIANCE_SERVER_[1-5] parameters can be used to designate servers for multistreaming or failover. Use the APPLIANCE_SERVER_LIST parameter to designate how these parameters are used.
Maximum length is 42 characters.

APPLIANCE_SERVER_LIST(MULTI_STREAM|FAILOVER|HOT_FAILOVER)

Set APPLIANCE_SERVER_LIST to *MULTI_STREAM* for a Guardium appliance connection to be established for each server that is identified by the APPLIANCE_SERVER_n or APPLIANCE_SERVER_FAILOVER_n parameters.

- If a connection is lost, S-TAP audit events continue to transmit over the remaining appliance connection.
- Lost connections are retried at regular intervals that are determined by multiplying the APPLIANCE_CONNECT_RETRY_COUNT by the APPLIANCE_PING_RATE.

Set APPLIANCE_SERVER_LIST to *FAILOVER* for one Guardium appliance connection to be active at a time.

- If the connection to the primary appliance is lost, a failover action occurs, which results in an attempt to connect to the next available server. The next available server is identified by the APPLIANCE_SERVER_n or APPLIANCE_SERVER_FAILOVER_n parameter.
- After a failover action occurs, the connection to the primary server is retried at regular intervals that are determined by multiplying the APPLIANCE_CONNECT_RETRY_COUNT by the APPLIANCE_PING_RATE.

Set APPLIANCE_SERVER_LIST to *HOT_FAILOVER* to keep each connected Guardium appliance active via pings. If the primary Guardium appliance (which is set by the APPLIANCE_SERVER parameter) becomes unavailable and failover occurs, *HOT_FAILOVER* maintains the activity of the primary appliance policy.
With all settings of APPLIANCE_SERVER_LIST, if all connections fail, and a spill file is specified (parameter OUTAGE_SPILLAREA_SIZE), events are buffered to the spill file until a connection becomes available. If no spill file is specified, and all connections are lost, data loss occurs.
The default is *FAILOVER*.

AUDIT

Specify a character string from one through 26 characters that defines the name of this IBM Guardium S-TAP for Data Sets agent.
There is no default.

CICS_SUPPORT

Enabling CICS® Transaction Server support activates additional reporting of CICS-specific information on record level events, including:

- CICS File ID
- CICS Function Code
- CICS Program ID
- CICS Region ID
- CICS Terminal ID
- CICS Transaction ID
- CICS User ID
- CICS Logical Unit of Work

Enable or disable CICS support by specifying `ENABLE` or `DISABLE`.
The default is *DISABLE*.
If you enable CICS support, you must also configure CICS for record level monitoring events to be captured for CICS. For more information about CICS support, see CICS Transaction Server support.

FORCE_LOG_LIMITED

Record level monitoring enables you to monitor VSAM file access based on key values. The VSAM key can contain Personally Identifying Information, such as account number, last name, or Social Security number. When the FORCE_LOG_LIMITED option is enabled, IBM Guardium S-TAP for Data Sets does not monitor any record level data. If the file is being monitored by a policy, then only file access is reported; monitoring and reporting of access to specific keys is suppressed.
Specify *Y* to prevent Personally Identifiable Identification (PII) data from being sent to the Guardium system. Data that is sent as part of Record Level Monitoring and CICS is considered PII. This data will not be sent to the Guardium system if FORCE_LOG_LIMITED(*Y*) is specified.
The default is *N*.

IAM_SMF_RECORD_ID

If you are using Innovation Access Method (IAM) from Innovation Data Processing, you must provide product-specific information for your SMF data to be processed. IAM provides a unique user-specified record ID, which it writes during CLOSE processing. For IBM Guardium S-TAP for Data Sets to report this access, determine the user SMF record ID for IAM, and specify that value in the IBM Guardium S-TAP for Data Sets control data set IAM_SMF_RECORD_ID option.
IAM writes SMF statistical data to a user-defined SMF record ID. Specify a numeric value that identifies the SMF record identification number used by IAM.
For IAM installations, consult your IAM administrator to determine the appropriate numeric value to include with this parameter.
Note:

- For z/OS Version 2 Release 3 and later, valid values are 128 – 1151.
- For z/OS Version 2 Release 2 and earlier, valid values are 128 – 255.

There is no product default value; however, the SAMPLIB member AUVSOPTS includes a default specification of 201.

INTERNAL_BUFFER_SIZE

Specify the size of the internal buffer used.

To improve performance, data is stored in an internal buffer that is sent when the buffer is full or during a ping request. If the buffer reaches the INTERNAL_BUFFER_SIZE, data is sent without waiting for the next ping request.

Specifying an INTERNAL_BUFFER_SIZE value that is too large for your environment can cause connection problems that are due to timing out while trying to send a large amount of data. Specifying too small a value might cause unnecessary I/O requests.

Tip: Performance varies based on system load, network load, and the load on the Guardium system, so the correct value for your environment cannot be predetermined. Begin with the default value, and make minor, incremental adjustments to improve performance, if necessary.

Valid values are 0 -- 2047 megabytes. The default is 8.

INITIAL_RULEDEF

You must not change this subsystem option unless IBM Software Support instructs you to do so. If instructed to modify this subsystem option, specify the name of the rule definitions member to use at startup. The default rule definitions member name is RULEDEFS.

MEGABUFFER_COUNT

Specify the number of IBM Guardium S-TAP for Data Sets audit events that are buffered, prior to the product attempting a TCP/IP send operation.

The megabuffer is flushed when either of two conditions is met:

- At regular intervals, based on the APPLIANCE_PING_RATE
- When the number of audit events that are held in the megabuffer reaches the count that is specified by this parameter

When MULTI_STREAM mode is enabled by parameter APPLIANCE_SERVER_LIST, and a megabuffer flush occurs, the audit event data stream is switched to the next available Guardium appliance. The event data stream will switch from appliance to appliance in a round-robin sequence as each megabuffer is sent.

Valid values are 1 -- 8192. The default is 200.

OUTAGE_SPILLAREA_SIZE

Specify the size of the spill file to be used when a connection cannot be made.

If the product includes a spill file, and no secondary APPLIANCE_SERVER_FAILOVER address is specified, or none of the secondary APPLIANCE_SERVER_FAILOVER addresses respond, it writes to the spill file. The spill file is meant for short-term outages only, because when a connection is restored to any Guardium system, it clears the spill file content before continuing to send data.

Valid values are 0 -- 1024 megabytes. If a valid value is not specified, a spill file is not created.

PREFER_IPV4_STACK

Specify the request for an IPV4 address to be issued from the Domain Name Server (DNS). The default value is N.

- Y causes a request to be issued to the DNS for an IPV4 address for the hostname that is specified in the APPLIANCE_SERVER parameter:
  - The DNS lookup request for an IPV4 address is attempted. If an IPV4 address is defined for the hostname, the DNS will respond with the value that will be used to connect to the Guardium appliance.
  - If only an IPV6 address is defined at the DNS, then the DNS will respond with the IPV6 address that will be used to connect to the Guardium appliance.
  - If both IPV4 and IPV6 addresses are defined at the Guardium appliance, the DNS will respond with both addresses, and the IPV4 address will be used to connect to the appliance.
- N or omitting this option from configuration causes a request for an IPV6 address to be issued to the DNS for the hostname that is specified by the APPLIANCE_SERVER parameter.
  - The DNS lookup request for an IPV6 address is attempted. If an IPV6 address is defined for the hostname, the DNS will respond with the value that will be used to connect to the Guardium appliance.
  - If only an IPV4 address is defined at the DNS, then the DNS will respond with the IPV6 address that will be used to connect to the Guardium appliance.
  - If both IPV4 and IPV6 addresses are defined at the Guardium appliance, the DNS will respond with both addresses, and the IPV4 address will be used to connect to the appliance.

Note: Whether or not this option is specified, if the address returned from the DNS is not valid for the hostname, it will result in failure to connect to the appliance, and the IBM Guardium S-TAP for Data Sets started task will terminate.

RLM

Specify the initial status of RLM processing by setting the RLM parameter to either *ENABLE* or *DISABLE*. *ENABLE* enables record level monitoring. *DISABLE* disables record level monitoring.

The default value is *ENABLE*.

SOCKET_CONNECT_TIMEOUT

Specify the length of time for socket connection attempts before failure or timeout.

Setting this value too low results in connection failures when the Guardium system is slow to respond. Setting this value too high causes problems in failover scenarios.

Tip: Performance varies based on system load, network load, and the load on the Guardium system, so the correct value for your environment cannot be predetermined. Begin with the default value, and make minor, incremental adjustments to improve performance, if necessary.

Valid values are 1 -- 65535. The default value, in seconds, is 3.

STAP_STREAM_EVENTS

Specify the initial streaming status by setting the STAP_STREAM_EVENTS parameter to either *Y* or *N*.

- Y indicates that the IBM Guardium S-TAP for Data Sets agent address space will send data to the server in a manner that is consistent with the active policy.
- N indicates that the agent address space will not send data to the server. It will perform all data collection processing in a manner that is consistent with the active policy. The agent address space will issue message AUV1070I at startup: TCP/IP STREAMING DISABLED DUE TO USER SETTING. See Simulation mode for more information.

The default value is *Y*.

SUBSYS

Choose any four-character alphanumerical subsystem ID to identify this particular instance of IBM Guardium S-TAP for Data Sets. For example, `AUV1`, `AUV2`, and so on.

Choose a unique SSID for each agent.

The default subsystem ID is *VTAP*.

SUPPRESS_INCOMPLETE_EVENTS

Enables SMF records without identifying characteristics to either be suppressed or sent to the appliance. Specify the SMF event filtering preference for SMF records with missing identifying characteristics, where:

- *N* indicates that missing field values in SMF records should always pass policy rule filters.
- *Y* indicates that missing field values should not pass the filters and the corresponding events should not be sent to the appliance.

The default value is *N*.
For more information, see SMF record identification considerations.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Configuring the started task JCL

You must configure the started task JCL statements with values that provide the system with information that is specific to your environment. Follow these steps to configure the started task JCL.

About this task

The IBM Guardium S-TAP for Data Sets started task JCL is located in the AUVJSTC member of the IBM Guardium S-TAP for Data Sets sample library (SAUVSAMP).
Note: Do not start the started task until you finish configuring IBM Guardium S-TAP for Data Sets. Attempting to start the started task before completing configuration can cause the started task to fail.

Procedure

1. Copy the IBM Guardium S-TAP for Data Sets started task JCL to your system PROCLIB from sample data set member AUVJSTC.
   Tip: Name the IBM Guardium S-TAP for Data Sets started task member AUVSTAPV. This name is easily identifiable with the IBM Guardium S-TAP for Data Sets product.
2. Verify that the statement: //AUVSTAPV PROC OPTSMBR=OPTIONS points to the default member name OPTIONS.
   The default member name OPTIONS was created during creation of the control data set.
3. Configure the started task JCL that you copied to your system PROCLIB by replacing AUV.V10R1M3 with the high-level qualifier of the installed IBM Guardium S-TAP for Data Sets load library.
   Note: For operation of the product, policy activation, and correct processing of data, the following conditions must be met:
   - A DD statement with the DDNAME OPTIONS must be in the IBM Guardium S-TAP for Data Sets started task. This DD statement points to the subsystem OPTIONS member of the IBM Guardium S-TAP for Data Sets control data set, which contains the global settings for the product. When the started task is initiated, it references the data in the subsystem options member to establish global settings, including the subsystem identifier for this specific instance of IBM Guardium S-TAP for Data Sets.
     - By default, the OPTIONS DD statement uses the same data set as the RULEDEFS and RULEDEFB DD statements. If necessary, you can specify a different data set for the OPTIONS DD statement other than that which is used for the DD statements RULEDEFS and RULEDEFB. The OPTIONS member must be present in the data set that is specified for the OPTIONS DD statement.
   - A DD statement with a DDNAME of CONTROL must be in the IBM Guardium S-TAP for Data Sets started task. For example: //CONTROL DD DSN=AUV.V10R1M3.CONTROL,DISP=SHR. This DD statement points to the IBM Guardium S-TAP for Data Sets control data set that contains the collection policy in the RULEDEFS member.
   - The two DD statements with the DDNAMES RULEDEFS and RULEDEFB must be present and must point to the same control data set name that was specified in the CONTROL DD statement. The member names RULEDEFS and RULEDEFB must not be changed. If DDNAMES RULEDEFS and RULEDEFB are not present, are changed, or do not point to the correct data set name, then the agent does not initiate correctly and is unable to collect data.
   - The high-level qualifier you specify for the control data set JCL when allocating the control data set must match the high-level qualifier you specify in the started task JCL.
   - The started task must have the authority to read and update the control data set and load library.
4. After you configure the started task JCL, add it to the z/OS® PROCLIB data set for started task initiation.
   Note:

   IBM Guardium S-TAP for Data Sets accommodates the use of multistream and improves support for large policies by providing a default started task JCL region size of 96 megabytes. When multistream is enabled, a buffer is created for each appliance, based on the INTERNAL_BUFFER_SIZE value. (Valid values are 0 - 2047 megabytes. The default value is 8.) The default started task JCL region size of 96 megabytes can accommodate large policies by providing space for up to six connected appliances with a default INTERNAL_BUFFER_SIZE of 8 megabytes and approximately 150,000 values in a policy.

   You might need to increase the started task JCL region size if:
   - the value specified for INTERNAL_BUFFER_SIZE is greater than 8 megabytes
   - an installed policy contains more than 150,000 values

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

CICS Transaction Server support

IBM Guardium S-TAP for Data Sets CICS® Transaction Server support enables you to filter and capture CICS transaction information.

IBM Guardium S-TAP for Data Sets must be running before CICS is started. If changes to a policy are made while a CICS file is open, the file must be closed and reopened for RLM-related policy changes to take effect.

Verify that the agent is running and correctly configured, and the appropriate work area storage is available.

- To capture data on files that are referenced within a transaction, the IBM Guardium S-TAP for Data Sets agent must be running and correctly configured to monitor each system image on which data sets reside.
- CICS support uses the XFCFROUT Global User Exit (GLUE).
- The GLUE acquires an above-the-line work area from the extended CICS dynamic storage area (ECDSA) of approximately 1412 bytes for each active or suspended transaction that performs at least one VSAM file operation. The work area is released at the end of the transaction.

- **Configuring CICS Transaction Server support**
  For CICS related information to be captured, you must configure CICS Transaction Server support.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Configuring CICS Transaction Server support

For CICS® related information to be captured, you must configure CICS Transaction Server support.

About this task

If you configure CICS Transaction Server support, you can capture CICS transaction information that is associated with record level monitoring of logical record activities that occur within a CICS transaction for KSDS and RRDS data sets. Remember to start IBM Guardium S-TAP for Data Sets before starting CICS. If changes to a policy are made while a CICS file is open, the file must be closed and reopened for any RLM-related policy changes to take effect.

Procedure

1. Configure the CICS system options.
   a. Specify the CICS_SUPPORT=ENABLE option, by using the subsystem options that are located in the OPTIONS member of the control data set.
2. Configure the CICS system initialization and system termination program list tables (PLTs), as shown in the example at the end of this topic.
   a. Enter the program AUVPLTPI after the DFHDELIM PLT entry.
   b. Enter the program AUVPLTPS before the DFHDELIM PLT entry.
   c. After creating or modifying the CICS system initialization and system termination PLTs, you must assemble and link them. For more information about creating a PLT, see the CICS Transaction Server for z/OS® Resource Definition Guide.
3. Specify autoinstall in the CICS system initialization parameters to automatically install the AUVPLTPI, AUVPLTPS, and AUVFROUT programs.
   If you do not specify autoinstall in the CICS system initialization parameters, you must define AUVPLTPI, AUVPLTPS, and AUVFROUT in the CICS system definition file (CSD). To install the program definitions in batch, sample JCL has been provided in member AUVCSDUP of the IBM Guardium S-TAP for Data Sets SAUVSAMP library that can be modified and used for the CICS program DFHCSDUP. Alternatively, the CICS CEDA Resource Definition Online transaction can also be used to perform the install of the program definitions. See the CICS Transaction Server for z/OS Resource Definition Guide for more information about installing resource definitions.
   a. Define the following attributes:
      - LANGUAGE (ASSEMBLER)
      - STATUS (ENABLED)
      - CEDF (NO)
      - DATALOCATION (BELOW)
      - EXECKEY (CICS)
      - EXECUTIONSET (FULLAPI)
      - RELOAD (NO)

      For the load modules to be located, the AUVPLTPI, AUVPLTPS, and AUVFROUT programs must be located in a load library located in the CICS DFHRPL concatenation within the CICS startup JCL.
4. Optional: The CICS facilities that implement RLM support, outside of normal CICS PLT initialization, can be enabled and disabled. To do so, define CICS transactions accordingly by using the batch CICS program DFHCSDUP or the CICS CEDA Resource Definition Online transaction.

   To enable the CICS facilities that are used to implement CICS RLM support, the following attributes must be assigned to the transaction:

   - TRANSACTION (*tran*, where *tran* is your chosen transaction ID)
   - PROGRAM (AUVPLTPI)
   - TASKDATAKEY (CICS)
   - TASKDATALOC (ANY)

   To disable the CICS facilities that are used to implement CICS RLM support, the following attributes must be assigned to the transaction:
   - TRANSACTION (*tran*, where *tran* is your chosen transaction ID)
   - PROGRAM (AUVPLTPS)
   - TASKDATAKEY (CICS)
   - TASKDATALOC (ANY)
5. Reference the program initialization and termination PLTs in parameters PLTPI and PLTPSD, as described in the topic, Using CICS system initialization parameters.

Results

If you have configured CICS support, message AUV3004I is displayed during CICS initialization to indicate that the Global User Exit AUVPLTPI XFCFROUT was installed and enabled.

Example

Enter the program AUVPLTPI after the DFHDELIM PLT entry in the CICS system initialization PLT:

```
*
*   CICS PROGRAM LIST TABLE FOR CICS SYSTEM INITIALIZATION
*
         DFHPLT TYPE=INITIAL,SUFFIX=I1
*
*  ENTRIES AHEAD OF DFHDELIM ARE EXECUTED IN FIRST PASS OF PLTPI
*  DURING THE SECOND PHASE OF CICS SYSTEM INITIALIZATION
*
         DFHPLT TYPE=ENTRY,PROGRAM=DFHDELIM
*
*  ENTRIES AFTERF DFHDELIM ARE EXECUTED IN SECOND PASS OF PLTPI
*  DURING THE THIRD PHASE OF CICS SYSTEM INITIALIZATION
*
         DFHPLT TYPE=ENTRY,PROGRAM=AUVPLTPI
*
         DFHPLT TYPE=FINAL
*
         END
```

Enter the program AUVPLTS before the DFHDELIM PLT entry in the CICS system termination PLT:

```
*
*   CICS PROGRAM LIST TABLE FOR CICS SYSTEM TERMINATION
*
         DFHPLT TYPE=INITIAL,SUFFIX=T1
*
```

```
*  ENTRIES AHEAD OF DFHDELIM ARE EXECUTED IN FIRST PASS OF PLTPSD
*  DURING THE FIRST PHASE OF CICS SYSTEM TERMINATION
*
       DFHPLT TYPE=ENTRY,PROGRAM=AUVPLTPS
*
       DFHPLT TYPE=ENTRY,PROGRAM=DFHDELIM
*
*  ENTRIES AFTERF DFHDELIM ARE EXECUTED IN SECOND PASS OF PLTSD
*  DURING THE SECOND PHASE OF CICS SYSTEM TERMINATION
*
*
        DFHPLT TYPE=FINAL
*
        END
```

- **Using CICS system initialization parameters**
  If you created program initialization and termination program list tables to use with IBM Guardium S-TAP for Data Sets, they must be referenced in the CICS system initialization parameters PLTPI and PLTSD.

Parent topic: CICS Transaction Server support

Using CICS system initialization parameters

If you created program initialization and termination program list tables to use with IBM Guardium S-TAP for Data Sets, they must be referenced in the CICS® system initialization parameters PLTPI and PLTSD.

- The suffix of the table that was created as the program initialization PLT must be referenced in the PLTPI parameter.
- The suffix of the table that was created as the program termination PLT must be referenced in the PLTSD parameter.

Here is a sample set of system initialization parameters that specifies the PLTPI and PLTSD suffixes:

```
AICONS=YES,
XRF=NO,
AUXTR=OFF,
AUXTRSW=NO,
APPLID=CICSSYSA,
FCT=NO,
    ...
PLTPI=I1,
PLTSD=T1,
    ...
SYSIDNT=SYSA
```

Parent topic: Configuring CICS Transaction Server support

Configuring CICS signon reporting

IBM Guardium S-TAP for Data Sets can identify the CICS® signon that was used for a specific file access event. Configure the product to enable the agent to send the CICS signon information to the Guardium system.

About this task

Remember: CICS signon records do not indicate a security failure. They are an indication that the identified user successfully accessed the named file or data set.
By default, IBM Guardium S-TAP for Data Sets reports only the CICS address SAF user ID for data set level events and failed security violations. However, for RACF® environments, both CICS and RACF can be configured for the S-TAP agent to report all of the following:

- the CICS signon
- the file or data set name that was accessed
- the access context (ALTER, CONTROL, UPDATE, or READ)

Note:

- Implementation of this facility requires changes to both CICS and RACF. After implementation, the resulting change to SMF type 80 processing results in the SMF80USR field containing the CICS signon for specific file accesses. Consult your CICS and RACF security administrator when considering the implementation of this facility.
- This facility does not report the data set activity, only the security level for the requested access event.
- The following steps are also documented in the *RACF Security Guide*. For more information, see the CICS Transaction Server for z/OS® RACF Security Guide.

To implement security for files managed by the CICS file control:

Procedure

1. Specify `RESSEC(YES)` in the CSD resource definition of the transactions that access the files.
2. Using the CICS file names for identification, define the profiles to RACF in the FCICSFCT or HCICSFCT resource classes, or their equivalent if you have a user-defined resource class names.
   a. For example, use the following commands to define files in the FCICSFCT class, and authorize users to read from or write to the files:

```
RDEFINE FCICSFCT (file1, file2, .., filen)
                UACC(NONE) NOTIFY(sys_admin_userid)
PERMIT file1 CLASS(FCICSFCT)
                ID(group1, group2) ACCESS(UPDATE)
PERMIT file2 CLASS(FCICSFCT)
                ID(group1, group2) ACCESS(READ)
```

3. To define files as members of a profile in the CICS file resource group class with an appropriate access list, use the following commands:

```
RDEFINE HCICSFCT (file_groupname)
               UACC(NONE) ADDMEM(filea, fileb, .., filez)
               NOTIFY(sys_admin_userid)
PERMIT file_groupname
               CLASS(HCICSFCT)
               ID(group_userid) ACCESS(UPDATE)
```

4. Specify `SEC=YES` as a CICS system initialization parameter, or `SECPRFX` if you define profiles with a prefix.
5. Specify `XFCT=YES` for the default resource class names of FCICSFCT and HCICSFCT, or XFCT=class_name for user-defined resource class names.

Results

RACF SMF type 80 records contain the CICS user signon in the SMF80USR field. The data is reported to the Guardium system records User ID field.
Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Starting the product

Start IBM Guardium S-TAP for Data Sets before starting products that perform similar functions.

Product initialization errors might occur if other products, which are known to intercept processing at the point of open, close, or record management functions for VSAM data sets, are started before IBM Guardium S-TAP for Data Sets. Message AUV1196E will warn you of a product initialization order conflict.

If you receive this error at startup:

1. Shut down IBM Guardium S-TAP for Data Sets and any similar products, including the previous version of this product
2. Close any data sets that are open under IBM Guardium S-TAP for Data Sets.
3. Start IBM Guardium S-TAP for Data Sets before starting similar products. IBM Guardium S-TAP for Data Sets must be running before CICS is started.

- **Starting and stopping the agent started task**
  Follow these steps to start and stop the IBM Guardium S-TAP for Data Sets agent started task.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Starting and stopping the agent started task

Follow these steps to start and stop the IBM Guardium S-TAP for Data Sets agent started task.

1. Start the agent started task by issuing the START command from the operator console, for example: START AUVSTAPV
2. Stop the agent started task by issuing the STOP command from the operator console, for example: STOP AUVSTAPV

You can configure the agent started task to start automatically during the z/OS® initial program load (IPL). To set automatic startup, add the appropriate command to the COMMNDxx member in SYS1.PARMLIB, or contact your system administrator.
Parent topic: Starting the product

Sample library members

The following sample library members are included for your use in installing and configuring IBM Guardium S-TAP for Data Sets. The following table lists them by type and description.

Table 1. Sample library members, types, and descriptions

Member	Type	Description
AUVCSDUP	JCL	Sample JCL to create CICS resource definition lists, groups, and program definitions with the CICS DFHCSDUP utility.
AUVJCNTL	JCL	Sample JCL to allocate and initially populate the control data set.
AUVJIVP	JCL	Sample JCL to verify installation.
AUVJSTC	JCL	Sample PROC to start the IBM Guardium S-TAP for Data Sets agent address space.
AUVSOPTS	Data	Initial data used to populate the control data set OPTIONS member.
AUVSRDEF	Data	Initial data used to populate the control data set RULEDEFS and RULEDEFB members.

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

Verifying the installation

After you install and configure the IBM® Guardium® S-TAP® for Data Sets agent, verify that the agent is properly installed. Use the JCL that is provided in the AUVJIVP member of the SAUVSAMP sample library.

Before you begin

Before you begin, complete all required tasks for Configuring the IBM Guardium S-TAP for Data Sets agent.

Procedure

1. You must install a policy on the IBM Guardium system with the characteristics listed below. Remember to replace <HLQ> with a valid high-level qualifier.

```
Job Name.....: AUVJIVP
Data Set Name: <HLQ>.AUVIVP.%%
DB Type......: DATA SET COLLECTION PROFILE
Data Set Type: ALL
```

```
Data Set Event: ALL
Actions......: z/OS AUDIT
```

Note: To see specific records on the IBM Guardium system, you might need to install a policy on the appliance in the first position that specifies Actions: LOG FULL DETAILS WITH VALUES.

2. Create a query on the IBM Guardium system that will report the events received from IBM Guardium S-TAP for Data Sets. Query characteristics are as follows:

```
Domain........: Access
Main Entity...: FULL SQL
Recommended Fields: IMS/DATA SET Event time
IMS/DATA SET Job Name
IMS/DATA SET Step Name
IMS/DATA SET Program Name
IMS/DATA SET Previous DSN
IMS/DATA SET Set Type
IMS/DATA SET Context
```

3. Start the IBM Guardium S-TAP for Data Sets started task.
4. Verify that the required SMF record types are enabled. Message AUV1450W in the Data Sets agent JESMSGLG log will alert you if any SMF record types are not defined.
5. Verify that the IBM Guardium S-TAP for Data Sets agent is connected to the intended appliance. Message AUV2182I in the Data Sets agent JESMSGLG log indicates a successful connection between the agent and the appliance.
6. Make the following modifications to the installation verification JCL in SAUVSAMP member AUVJIVP:
   a. Add a valid job card.
   b. Replace all occurrences of <HLQ> with the same high-level qualifier that was used in the policy as described in Step 1.
7. Submit the modified JCL in SAUVSAMP member AUVJIVP.

Results

Verify that the following data sets contexts appear on the appliance:

Table 1. Data set contexts for installation verification

Step	Description	Data set contexts
GENDATA	Generate input data for subsequent job steps	None
VSAM	Define, load, rename and delete ESDS, KSDS, and RRDS data sets	DATA SET ALTER DATA SET CLOSE DATA SET CREATE DATA SET DELETE DATA SET OPEN DATA SET RENAME DATA SET UPDATE
PDS	Create a PDS and write to a new PDS member	DATA SET CLOSE DATA SET CREATE Member Add
PDSCOPY	Copy a PDS member to another PDS member	DATA SET CLOSE Member Add
PDSREPL	Copy over an existing PDS member	DATA SET CLOSE Member Replace
PDSTEST	Rename a PDS member, create an alias, delete all PDS members, rename the PDS, and delete the PDS	DATA SET CLOSE DATA SET DELETE DATA SET RENAME Member Add Member Delete Member Rename STOW Initialize

Parent topic: Configuring the IBM Guardium S-TAP for Data Sets agent

IBM Guardium S-TAP for Data Sets administration

You must configure the Guardium system to communicate with the IBM Guardium S-TAP for Data Sets agent.

- **Communicating with the Guardium system**
  The Guardium system and the S-TAP for Data Sets agent need to communicate policy rules and collected data by using a TCP/IP connection. For the IBM Guardium S-TAP for Data Sets to communicate with the Guardium system, the following conditions must be met:
- **Communicating with the IBM Guardium S-TAP for Data Sets started task**
  IBM Guardium S-TAP for Data Sets operator commands enable authorized users to perform selected operations. Several types of operator commands can be used to display the status of IBM Guardium S-TAP for Data Sets, to enable and disable certain functions, and to dynamically alter processing without stopping or quiescing the product.

- **Data collection**
  IBM Guardium S-TAP for Data Sets collects data from multiple sources. This section describes the data collection process, as well as filtering stages and their performance impacts.
- **Record level and SMF data set monitoring options**
  You can reduce z/OS CPU and storage usage by setting options for Record level and SMF data set monitoring.
- **Policy pushdown**
  Policy pushdown is a method of controlling the data that is collected by the IBM Guardium S-TAP for Data Sets agent. Policy pushdown enables the agent to evaluate the filtering criteria that you specified.
- **Data set collection filtering parameters**
  Use the following filtering parameters to collect data set event data.
- **CICS collection filtering parameters**
  Use the following filtering parameters to collect transaction data from CICS®.

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS

Communicating with the Guardium system

The Guardium system and the S-TAP for Data Sets agent need to communicate policy rules and collected data by using a TCP/IP connection. For the IBM Guardium S-TAP for Data Sets to communicate with the Guardium system, the following conditions must be met:

- The IBM Guardium S-TAP for Data Sets TCP/IP connection must be configured.
- At least one agent per z/OS® image must be specified. When you are configuring an agent instance:
  - Specify the host name or IP address on which the Guardium system is running. This value is specified by the APPLIANCE_SERVER element in the agent configuration file. The complete name of this CONTROL member is OPTIONS.

  When the agent is started, it uses the specified configuration information to connect to the Guardium system.

- **Streaming audit data to multiple systems**
  Multistream mode enables S-TAP audit events to be sent to multiple connected appliances. You can enable multistreaming to up to 6 Guardium appliances (APPLIANCE_SERVER + APPLIANCE_SERVER_*n*, where *n* can be 1 - 5).
- **Keeping connections active when HOT_FAILOVER is enabled**
  When the *HOT_FAILOVER* feature is enabled by the APPLIANCE_SERVER_LIST parameter, each connected Guardium appliance is kept active via pings.

Parent topic: IBM Guardium S-TAP for Data Sets administration

Streaming audit data to multiple systems

Multistream mode enables S-TAP audit events to be sent to multiple connected appliances. You can enable multistreaming to up to 6 Guardium appliances (APPLIANCE_SERVER + APPLIANCE_SERVER_*n*, where *n* can be 1 - 5).

IBM Guardium S-TAP for Data Sets sends events to a single appliance until a ping occurs, or the number of records that is specified by MEGABUFFER_COUNT is reached.

To enable multistreaming, you must specify *MULTI_STREAM* when you configure the APPLIANCE_SERVER_LIST parameter in the OPTIONS member of the CONTROL data set. Parameters APPLIANCE_SERVER and APPLIANCE_SERVER_[1-5] specify the appliances to which you intend to stream events. The appliance that is specified by APPLIANCE_SERVER provides the policy that is used for event matching.

For more information about OPTIONS member parameters, see Specifying subsystem options.

Parent topic: Communicating with the Guardium system

Keeping connections active when HOT_FAILOVER is enabled

When the *HOT_FAILOVER* feature is enabled by the APPLIANCE_SERVER_LIST parameter, each connected Guardium appliance is kept active via pings.

If the primary appliance becomes unavailable and failover occurs, the appliance policy that was originally pushed from the primary appliance continues to be active. When all Guardium appliances are connected, the status of each appliance connection, listed in the Guardium interface, is green.

Parent topic: Communicating with the Guardium system

Communicating with the IBM Guardium S-TAP for Data Sets started task

IBM Guardium S-TAP for Data Sets operator commands enable authorized users to perform selected operations. Several types of operator commands can be used to display the status of IBM Guardium S-TAP for Data Sets, to enable and disable certain functions, and to dynamically alter processing without stopping or quiescing the product.

- **IBM Guardium S-TAP for Data Sets started task commands**
  If you are an authorized user, you can enter commands to display the status of IBM Guardium S-TAP for Data Sets enable and disable certain functions, and dynamically alter processing without shutting down or quiescing the system.

Parent topic: IBM Guardium S-TAP for Data Sets administration

IBM Guardium S-TAP for Data Sets started task commands

If you are an authorized user, you can enter commands to display the status of IBM Guardium S-TAP for Data Sets enable and disable certain functions, and dynamically alter processing without shutting down or quiescing the system.

Commands

Enter operator commands from an MVS™ operator console, or by using a facility that issues MVS commands, such as SDSF.

The command format is MODIFY*stcname*, where *stcname* is the name of the started task, followed by the DISPLAY command.

For example, for record level monitoring, you can enter: MODIFY*stcname*,DISPLAY RLM. You can also use the shorthand for MODIFY, which is F to enter F*stcname*,DISPLAY RLM.

The following table summarizes the commands for displaying monitoring status and for enabling or disabling monitoring:

Table 1. Started task commands and descriptions

Command	Description
DISPLAY RLM	Indicates whether record level monitoring is enabled or disabled
DISPLAY SMFM	Indicates whether SMF monitoring is enabled or disabled
ENABLE RLM	Enables record level monitoring
DISABLE RLM	Disables record level monitoring
ENABLE SMFM	Enables SMF monitoring
DISABLE SMFM	Disables SMF monitoring
DISPLAY STREAM	Indicates whether audit records are being sent to the appliance
DIAG	Displays diagnostic information about the agent. Also displays the counters, which record the number of SMF-based and RLM-based audit records that are created as well as the number of audit records that are sent to the appliance.

Parent topic: Communicating with the IBM Guardium S-TAP for Data Sets started task

Data collection

IBM Guardium S-TAP for Data Sets collects data from multiple sources. This section describes the data collection process, as well as filtering stages and their performance impacts.

Record level and SMF event monitoring

Event information is gathered at run time through record level and SMF event monitoring. For both record level and SMF event monitoring, the filtering options you specify can minimize overhead, and control the performance of the data collection and reporting phases of processing. IBM Guardium S-TAP for Data Sets uses the filtering criteria you define to dynamically tune its processing path for optimal performance.

With few exceptions, you can use the same filtering criteria for both record level and SMF event monitoring.

- Specify the minimal filtering criteria necessary for your policy. Filtering only on the data you require minimizes:
  - Data collection overhead
  - Event processing
  - Event reporting
  - CPU time
  - Memory usage

  Record level monitoring creates the potential for the collection and reporting of large amounts of data. When constructing a policy and specifying filtering criteria, carefully consider the potential amount of data to be collected and processed.
- In the user interface, you can specify lists of elements for some filters, and use generic characters (wildcards) to create more flexibility in your filtering criteria. Generic characters act as placeholders in the specification of a character-based operand, representative of one or more valid characters for the entity on which an operation is performed.
- The use of generic characters can reduce the total number of policy rules required, but an overly inclusive set of selected entities can ultimately reduce efficiency. Excessive use of generic characters can increase the scope of selectivity during the qualification of records for processing, and dramatically reduce efficiency and increase overhead.
- SMF event monitoring can be controlled at a higher level through the specifications in the SMFPRMxx z/OS® system PARMLIB member.

Note:

- Record level monitoring support for a data set is detected, filtered, and activated at OPEN time. Files that are open at the time of an initial or updated policy activation will not be intercepted for RLM processing unless the application permits closing and reopening the file. This is of particular importance for CICS, which typically opens files at initialization or at first-use of a file. If a policy is updated after a CICS file has already been opened, it must be closed and reopened to be eligible for RLM processing.
- Record level monitoring enables you to monitor VSAM file access based on key values. The VSAM key can contain Personally Identifying Information, such as account number, last name, or Social Security number. When the FORCE_LOG_LIMITED option is enabled, IBM Guardium S-TAP for Data Sets does not monitor any record level data. If the file is being monitored by a policy, then only file access is reported; monitoring and reporting of access to specific keys is suppressed.

Filtering stages

Both record level and SMF event monitoring are performed in stages. If a collected event does not pass the lowest filtering stage (0), further processing of that event is not performed. Otherwise, the event is reevaluated during the next stage of filter processing, and IBM Guardium S-TAP for Data Sets determines whether the event should be auditing and reporting.

Stage 0 filtering

Stage 0 filtering should only be used by advanced users. An understanding of each SMF record type is required.
Stage 0 filtering can be performed for SMF event monitoring only. Only SMF events being recorded by SMF can be monitored for processing.
SMF record types to be monitored must be defined in the SMFPRMxx z/OS System Initialization PARMLIB member. If one or more SMF record types to be monitored are not specified, data collection cannot be performed. See the *SMF record types collected by IBM Guardium S-TAP for Data Sets* section of this user's guide for

details on the record types and the associated data collected with each record type.

Stage 1 filtering

Stage 1 filtering can be performed with both record level and SMF event monitoring.
Filter out as much data as possible to achieve the best possible performance.
The filtering criteria specified in the policy associated with this level of filtering include:

- Data set name
- Data set type
- DD name
- Job name
- Job type
- Program name
- Security system user ID
- Security system group ID
- SMF system ID
- Subsystem ID
- Sysplex name
- VSAM record organization*

*VSAM record organization is only available as a filtering criterion for record level monitoring. Only key-sequenced data set (KSDS) and relative record data set (RRDS) organizations are supported.
Some of the possible filtering criteria for Stage 1 filtering include a wider scope of data than others. For example, a user ID can require a much larger subset of data for processing than a data set name requires. You can define the minimum amount of data to be monitored, collected, and reported on by including or excluding selection criteria, creating lists of elements, and specifying relational operators for most criteria.
Stage 1 filtering for record level monitoring: For record level monitoring, Stage 1 filtering occurs at OPEN time for KSDS and RRDS VSAM data sets.
Stage 1 filtering for SMF event monitoring: For SMF event monitoring, Stage 1 filtering occurs in the IBM Guardium S-TAP for Data Sets address space immediately after a monitored SMF record type is obtained by the collector, located at the SMF User Exit collection point.

Stage 2 filtering

Stage 2 filtering for record level and SMF event monitoring applies to the following event types:

- Data set open
- Data set close
- Data set create
- Data set alter
- Data set update
- Data set delete
- Data set rename
- Data set SAF alter
- Data set SAF control
- Data set SAF define
- Data set SAF read
- Data set SAF update
- Member add
- Member replace
- Member rename
- Member delete
- STOW initialize

Default or specified event types are collected and passed on to the Guardium system.
Stage 2 filtering for record level monitoring can be based on the type of logical record access as well as one or more values for the key of the VSAM data set. The types of record level access that can filtered on in Stage 2 are:

- Record insert
- Record delete
- Record update
- Record read

You can use a key value or list of key values, as well as a key range or list of key ranges, to further limit the amount and scope of data collected. The key data can be specified in normal printable characters or in hexadecimal by using the EBCDIC character set.
For key values, you can use generic characters in the specification of the keys. Only those records that pass Stage 2 filtering are collected and passed on to the Guardium system.
If CICS® support is enabled, you can filter the record level monitoring event data that is captured within a CICS transaction. CICS transaction data can be filtered by:

- CICS user ID
- CICS transaction ID
- CICS program ID
- CICS file ID
- CICS region ID
- CICS terminal ID
- CICS function code

Stage 3 filtering

Stage 3 filtering is performed by IBM Guardium S-TAP for Data Sets based on Stage 2 filtering criteria that you define. During policy pushdown and activation, an analysis of the policy filtering criteria is performed. This analysis enables prefiltering processing determinations that can be performed across the product. Stage 3 prefiltering can be very efficient in eliminating certain types of data collection, and ultimately reducing the path length through the product to provide optimal processing performance.
Examples:

- **Record level monitoring:** If no record level monitoring event types are specified in the policy, Stage 2 filtering is eliminated, which reduces overhead significantly.
- **SMF event monitoring:** The exclusion of certain SMF event monitoring types from your filtering criteria allows IBM Guardium S-TAP for Data Sets to bypass collection very early in the SMF User Exit data collection, and eliminates all downstream processing for that SMF record type.

Exclusions

IBM Guardium S-TAP for Data Sets does not collect information on the following types of activities:

On IBM Db2® subsystems
: Activity within address spaces whose STC names have the following endings:

- MSTR (example: QA1XMSTR)
- DIST (example: QA1XDIST)
- IRLM (example: QA1XIRLM)
- DBM1 (example: QA1XDBM1)

On IBM IMS subsystems
: Accesses performed by the following program names:

- DFSMVRC0
- CQSINIT0
- HWSHWS00
- IRTRRC00
- DFSRRC00
- DFSUARC0
- DSPCINT0
- DSPURI00

SMF record identification considerations

In certain cases, such as when an SMF record is generated before the issuing job is run, SMF records can have zeros in the fields that the agent uses for record identification. When this happens, the agent is unable to find a RULEDEFS match for the record by using this field or any dependent fields. To avoid data loss, the agent still sends these records to the appliance even if the policy rule is set to filter out those fields. If one or more identifying fields are empty, you can use the Guardium appliance to highlight them, for example, by marking them with a specific color. The data set audit fields that can be affected by this consideration are:

- Job name
- Job number
- Program name
- DD name
- User ID
- Group ID
- Job type
- Step name
- Step number

To optionally suppress incomplete events from being sent to the appliance, use the SUPPRESS_INCOMPLETE_EVENTS parameter as described in Specifying subsystem options.

Parent topic: IBM Guardium S-TAP for Data Sets administration

Record level and SMF data set monitoring options

You can reduce z/OS® CPU and storage usage by setting options for Record level and SMF data set monitoring.

Record level monitoring performance

During record level monitoring, data is collected when VSAM records are read or written. Record level monitoring can affect performance, TCP/IP traffic, and system load. Record level monitoring intercepts VSAM accesses at the record level, so excessive monitoring of logical record requests can result in large volumes of data being transferred to the Guardium system from the TCP/IP telecommunications link, along with a corresponding increase in CPU and storage use within z/OS. Even in a moderately-sized installation that uses VSAM files, hundreds of millions, if not billions, of logical record requests can be made to VSAM daily. Attempting to monitor and report on all VSAM requests can result in huge volumes of data that can increase system load on z/OS and data traffic on communication links.

To provide flexibility in controlling the impact of record level monitoring, policy options can be used to limit the scope of monitoring. Carefully consider these options with the goal of limiting record level monitoring to the logical record requests in specific data sets that must be monitored in your environment.

Record level monitoring filter options

You can use the record level monitoring to filter based on:

- Data set name
- Data set type
- Job name
- Job type
- Program name
- Security system user ID
- Security system group ID
- SMF system ID
- Subsystem ID
- Sysplex name
- VSAM record organization
- DD name

If CICS® support is enabled you can also filter based on:

- CICS user ID

- CICS transaction ID
- CICS program ID
- CICS file ID
- CICS region ID
- CICS terminal ID
- CICS function code

You can also limit the monitoring of records to particular keys or key ranges:

VSAM KSDS and RRDS data sets
: For KSDS data sets, the key used is defined when the data set is created through an IDCAMS DEFINE.
For RRDS data sets, the key is a relative record number within the data set.
For individual keys, a list of keys is permitted with which a comparison operator can be used. In situations where the key contains unprintable characters, you can define the keys or key ranges by using hexadecimal notation.

Limit the monitoring of record level requests by the type of logical requests, including:

- Record read events
- Update write events
- Insertions
- Deletions

Remember: Each monitored record that matches the various policy filters results in the processing, creation, and transmission of a record monitoring data element to the Guardium system. Use the Guardium system interface to establish as restrictive a set of policy filters as possible. IBM Guardium S-TAP for Data Sets dynamically tunes and minimizes processing based on the filtering criteria chosen. Effectively chosen filters allows for maximum efficiency of record level monitoring processing.

Activating record level monitoring

You must define a policy that includes rules that specify one or more of the record level request filters (reads, update writes, insertions, or deletions) in order to activate record level monitoring.

- If a policy does not contain any of these filters, no additional overhead occurs at the logical record request level.
- If a particular policy rule contains one or more of these filters, only the specific data set defined in the rule (or data sets associated with other policy filters defined in the rule) incurs any additional monitoring overhead.
- Record level monitoring is only valid for use with VSAM data sets (KSDS and RRDS only).

SMF data set monitoring performance and filtering

Use filtering criteria to limit the amount of VSAM data set monitoring to only particular events. By using policy filters, SMF data set monitoring performance is enhanced by reducing CPU usage, storage usage, and TCP/IP traffic to the Guardium system.

Filter down to each specific VSAM data set event with the following filters:

- Data Set Open
- Data Set Update
- Data Set Close
- Data Set Close (input-only)
- Data Set Close (output-only)
- Data Set Delete
- Data Set Rename
- Data Set Create
- Data Set Alter
- Data Set SAF Alter
- Data Set SAF Update
- Data Set SAF Read
- Data Set SAF Define
- Data Set SAF Control

Filter down to each specific non-VSAM data set event with the following filters:

- Data Set Close
- Data Set Close (input-only)
- Data Set Close (output-only)
- Data Set Delete
- Data Set Rename
- Data Set Create
- Data Set SAF Alter
- Data Set SAF Update
- Data Set SAF Read
- Data Set SAF Define
- Data Set SAF Control
- Member Add
- Member Delete
- Member Rename
- Member Replace
- STOW Initialize

You can achieve optimal record level monitoring and SMF data set monitoring performance when you create and use a policy that defines only those events that are required by your organization.

Parent topic: IBM Guardium S-TAP for Data Sets administration

Policy pushdown

Policy pushdown is a method of controlling the data that is collected by the IBM Guardium S-TAP for Data Sets agent. Policy pushdown enables the agent to evaluate the filtering criteria that you specified.

Evaluating a match

When the product is searching for a match for the filtering criteria that you have specified, an evaluation is performed through each data set level. Access rules are used for processing a data set, when the filtering criteria of the following access types match the data:

- Job name
- Program
- Data set name
- Data set type
- DD name
- User ID
- Group ID
- SYSPLEX
- SSID
- SYS ID
- RECORG*
- Job type

*RECORG is valid only for the processing of VSAM record level monitoring.
The following values are not used to evaluate for a match on an access rule. They are used as subfiltering criteria after a match on a data set is found:

- Key
- Key range
- Data set event
- RLM event
- CICS® user ID
- CICS transaction ID
- CICS program ID
- CICS file ID
- CICS region ID
- CICS terminal ID
- CICS function code

Multiple values are allowed in an access rule, as shown in the following example with two access rules:

```
Access Rule 1
    Rule Type = INCLUDE
    Job Name = JOBA
    Key = "111111"
    RLM Event = ALL
Access Rule 2
    Rule Type = INCLUDE
    Job Name = JOBA
    Key = "222222"
    RLM Event = ALL
```

When a match is found on Access Rule 1 for job JOBA, no further scanning of the Access Rules occurs. The keyword *Key* is not used as part of the Access Rule match. To filter on keys "111111" and "222222" for a job that is named JOBA, code the Access Rules as follows:

```
Access Rule 1
    Rule Type = INCLUDE
    Job Name = JOBA
    Key = "111111","222222"
    RLM Event = ALL
```

This rule searches for a match on the job name JOBA. If a match on JOBA is found, the RLM Event and Key values are matched.
Parent topic: IBM Guardium S-TAP for Data Sets administration

Data set collection filtering parameters

Use the following filtering parameters to collect data set event data.

All the fields are optional and most have a default behavior as described. All fields apply to both VSAM and non-VSAM monitoring, unless otherwise specified.

Rule Type
: Indicates whether this rule indicates inclusion or exclusion for events that match the criteria.
Allowed values are: INCLUDE|EXCLUDE: Include collects events that satisfy the specified criteria; exclude does not collect those events. If nothing is specified, then INCLUDE is used.

Job Type
: Indicates the type of jobs that should be considered for a match.
If nothing is specified, all types are collected. You can specify the following values, separated by a comma (,): JOB|STC|TSU|APPC|OMVS, where:

  JOB
  : Jobs

  STC

Started Task

TSU
: Time Sharing User

APPC
: Advanced Program-To-Program Communication

OMVS
: Open MVS access to non-VSAM data sets, particularly that performed by FTP

SYS ID
: Indicates the SMF System IDs to use when searching for a match.
1 - 4 character SMF System ID to match.
Can be optionally followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Valid wildcards are supported at any position. They are:

- Percent sign (%) for zero or more characters
- Question mark (?) for a single character match

If left blank, then all SMF System IDs are considered a match.
Examples:

SS01
: Matches events that occur on SS01

SS01,EQ
: Matches that occur on SS01

SS%,EQ
: Matches that occur on systems with SS as the first 2 characters in the SMF system ID

RECORG
: Indicates the record organization type to match.
Applies only to VSAM record level monitoring collection.
Can contain zero or more of the following values, separated by a comma (,): KSDS|RRDS, where:

KSDS
: Key-sequenced data set

RRDS
: Relative record data set

If left blank, all record organization types for record level monitoring are considered a match.
Examples:

KSDS
: Matches key-sequenced data set events

KSDS,RRDS
: Matches key-sequenced data set, and relative record data set events

User ID
: Indicates the user ID to use when searching for a match.
1 - 8 character user ID to match.
Can be optionally followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Wildcards are supported.
If left blank, then activities for all user IDs are considered a match.
Examples:

PDUSER01
: Matches events that are caused by user *PDUSER01*

PDUSER01,EQ
: Matches events that are caused by user *PDUSER01*

PDUSER%,EQ
: Matches events that are caused by users with the prefix *PDUSER*

SSID
: Indicates the AUV ID to use when searching for a match.
1 - 4 character AUV ID optionally followed by a comma (,) and a relational operator. If no relational operator is provided EQ is assumed.
Wildcards are supported.
If left blank, activities for all SSID are considered a match.
Examples:

AUV1
: Matches events from systems with AUV ID of AUV1

AUV1,EQ
: Matches events from systems with AUV ID of AUV1

AUV%,EQ
: Matches events from systems with AUV ID prefix of AUV

SYSPLEX
: Indicates the z/OS sysplex name to use when searching for a match.
The specific 1 - 8 character z/OS sysplex name, optionally followed by a comma (,) and a relational operator. If no relational operator is provided, EQ is assumed.
Wildcards are supported.
If left blank, then activities for all SYSPLEX are considered a match.
Examples:

SYSPLEX1
: Matches events from systems on SYSPLEX1

SYSPLEX1,EQ
Matches events from systems on SYSPLEX1
SYSPLEX%,EQ
Matches events from systems on a plex beginning with SYSPLEX

Program
Indicates the program name to use when searching for a match.
1 - 8 character program name, optionally followed by a comma (,) and a relational operator. If no relational operator is provided, EQ is assumed.
Wildcards are supported.
If left blank, activities from all programs are considered a match.
Examples:

IDCAMS
Matches events that are accessed from IDCAMS
IDCAMS,EQ
Matches events that are accessed from IDCAMS
IDCAM%,EQ
Matches events that are accessed from programs beginning with IDCAM

Group ID
Indicates the group ID to use when searching for a match.
1 - 8 character representing the security system group ID optionally followed by a comma (,) and a relational operator. If no relational operator is provided EQ is assumed.
Wildcards are supported.
If left blank, then activities from all groups are considered a match.
Examples:

GROUP1
Matches events that are caused by someone within GROUP1
GROUP1,EQ
Matches events that are caused by someone within GROUP1
GROUP%,EQ
Matches events that are caused by someone within a group ID beginning with GROUP

Data Set Name
Indicates the data set name to use when searching for a match.
1 - 44 character that represents the data set name for which activity is collected, optionally followed by the comma character (,) and a relational operator. If no relational operator is provided, EQ is assumed.
Wildcards are supported.
If left blank, all data set names are considered a match.
Examples:

HLQ1.MLQ1.LLQ1
Matches events on HLQ1.MLQ1.LLQ1
HLQ1.MLQ1.LLQ1,EQ
Matches events on HLQ1.MLQ1.LLQ1
HLQ%.MLQ%.LLQ%.EQ
Matches events with the data set name mask HLQ%.MLQ%.LLQ%
%.%%,EQ
Matches all data sets with more than one qualifier
%,EQ
Matches all data sets with one qualifier

DD Name
Indicates the DD name to use when searching for a match.
1 - 8 character DD name, optionally followed by a comma (,) and a relational operator. If no relational operator is provided, EQ is assumed.
Wildcards are supported.
If left blank, activities for all DD names are considered a match.
Examples:

PAYFILE
Matches events that are accessed by DD name *PAYFILE*
PAYFILE,EQ
Matches events that are accessed by DD name *PAYFILE*
PAYFIL%,EQ
Matches events that are accessed by DD names beginning with *PAYFIL*

Job Name
Indicates the job name to use when searching for a match.
1 - 8 character name representing the job for which activity must be collected, optionally followed by a comma (,) and a relational operator. If no relational operator is provided, EQ is assumed.
Wildcards are supported.
If left blank, then activities from all jobs are considered a match.
Examples:

AUVJOB01
Matches events that result from a job name AUVJOB01
AUVJOB01,EQ
Matches events that result from a job name AUVJOB01
AUVJOB%,EQ
Matches events that result from any job beginning with AUVJOB

Key

Indicates the keys to consider when searching for a match.
Only applies to VSAM record level monitoring collection.
One or more keys in plain text or hexadecimal format, representing the key for which to match event data during record level monitoring processing.
Multiple keys must be delimited by a comma (,) optionally followed by the comma character (,) and a relational operator. If no relational operator is provided, EQ is assumed.
Plain text keys can be 1 - 255 characters long.
Hexadecimal keys can be 2 - 510 characters long and must always have an even number of characters.
An individual key must be surrounded in double quotation marks ("").
If the key is in hexadecimal format, it must be prefixed with x' and suffixed with a single quotation mark (') . It must be placed inside double quotation marks, for example: "x'F0F0F1'"
A backslash (\) can precede any character to escape the character. For example:

`"\x'0123'"`
: Matches the plain text key "x'0123'" instead of a hexadecimal key. Both types can be supplied together.

Wildcards are supported. If a wildcard is supplied with a hexadecimal key, the wildcard must be in hexadecimal (6C for `'%'`, 6E for `'?'`).
If a provided key is greater than the actual length of the VSAM key, the key will be truncated. If the key provided is shorter than the VSAM key, it will be padded with hex zeroes.
If the Key and Key Range fields are blank, activities for all keys are considered a match.
Examples:

`"KEY01"`
: Matches record level monitoring events with a key of KEY01

`"KEY01","KEY02"`
: Matches record level monitoring events with a key of KEY01 or KEY02

`"x'F0F0'"`
: Matches record level monitoring events with a key that contains the hexadecimal value F0F0

`"x'F0F0'","x'F0F1'"`
: Matches record level monitoring events with a key that contains the hexadecimal value of F0F0 or F0F1

`"KEY01","x'F0F1'"`
: Matches record level monitoring events with a key of KEY01 or a key with the hexadecimal value of F0F1

`"KEY0%"`
: Matches record level monitoring events with a key beginning with KEY0.

`"x'F06C'″`
: Matches record level monitoring events with a key with a hexadecimal value beginning with F0

`"\x'F06C'″`
: Matches record level monitoring events with a key of x'F06C'

Key Range

Indicates the range of keys to consider when searching for a match.
Only applies to VSAM record level monitoring collection.
A pair of keys in plain text, or a pair of keys in hexadecimal, representing the range to match for record level monitoring. This must be specified as <key1>,<key2>.
A pair of keys must both be in plain text, or both be in hexadecimal. Each plain text key in a plain text key pair can be 1 - 255 characters long. Each hexadecimal key in a hexadecimal key pair can be 2 - 510 characters long and must have an even number of characters.
If the keys are in hexadecimal, they must begin with x' and end with a single quotation mark (') . All keys must be enclosed in double quotation marks.
A backslash (\) can precede any characters to escape the character.
There must be an even number of keys in this field.
All key pairs must have the smaller key in the first value and the larger key in the second value; otherwise the key pairs will be rejected.
Wildcards are not supported in this field.
If the provided key is greater than the actual length of the VSAM key, the provided key will be truncated. If the key provided is shorter than the VSAM key, it will be padded with hex zeroes.
If the Key Range and Key fields are blank, activities for all keys are considered a match.
Examples:

`"KEY01","KEY09″`
: Matches record level monitoring events where the key is between KEY01 and KEY09

`"KEY01","KEY09","KEY11","KEY19″`
: Matches record level monitoring events where the key is between KEY01 and KEY09 or between KEY11 and KEY19

`"x'F0F0'","x'F0F9'″`
: Matches record level monitoring events where the key has a hexadecimal value between F0F0 and F0F9

`"x'F0F0'","x'F0F9'","x'F1F0'","x'F1F9'"`
: Matches record level monitoring events where the key has a hexadecimal value between F0F0 and F0F9 or between F1F0 and F1F9

`"\x'F0F0'","\x'F0F9'″`
: Matches record level monitoring events where the key is between x'F0F0' and x'F0F9'

RLM Event

Indicates what type of record level monitoring events should be considered for a match.
Only applies to VSAM record level monitoring collection.
Must contain zero or more of the following values, separated by a comma (,): RINS|RDEL|RWRT|RGET|ALL|SKIP, where:

RINS
: A record insert within a data set of a supported type

RDEL
: A record delete within a data set of a supported type

RWRT
: A record level update within a record of a supported type

RGET
: A record level that is read within a data set of a supported type

ALL

: Returns all record level events

SKIP

Returns no record level events

If left blank, then SKIP is the default and nothing is considered a match
Examples:

RINS
: Matches record level monitoring events where the operation was a record insert

RINS,RDEL
: Matches record level monitoring events where the operation was a record insert or a record delete

Data Set Event
: Indicates what type of SMF Data Set Events should be considered for a match.
Must contain zero or more of the following values, separated by a comma (,):

```
DSCLI | DSCLO | DSOP | DSCL | DSUP | DSDL | DSRN | DSCR | DSALT | DSRAL | DSRCN | DSRRD |
DSRUP | DSRDF | MADD | MREP | MREN | STOWI | ALL | SKIP
```

where:

DSOP
: An OPEN event against a supported data set type

DSCL
: A CLOSE event against a supported data set type

DSCLI
: A CLOSE event against a supported data set type that was opened for input

DSCLO
: A CLOSE event against a supported data sets type that was opened for output

DSUP
: An UPDATE event against a supported data set type

DSDL
: A DELETE event against a supported data set type

DSRN
: A RENAME event against a supported data set type

DSCR
: A DEFINE or NEW ALLOCATION event of a supported data set type

DSALT
: An ALTER of the attributes of a supported data set type

DSRAL
: A security facility ALTER access of a supported data set type

DSRCN
: A security facility CONTROL access of a supported data set type

DSRRD
: A security facility READ access of a supported data set type

DSRUP
: A security facility UPDATE access of a supported data set type

DSRDF
: A security facility DEFINE access of a supported data set type

MADD
: A member add event against a supported data set type

MREP
: A member replace event against a supported data set type

MREN
: A member rename event against a supported data set type

MDEL
: A member delete event against a supported data set type

STOWI
: A STOW initialize event against a supported data set type

ALL
: Returns all data set level events

SKIP
: Returns no data set level events

If left blank, ALL is the default and all types are considered a match.
Examples:

DSOP
: Matches data set events where an open occurred.

DSOP,DSCL
: Matches data set events where an open or a close occurred.

Valid relational operators are:

- EQ (Equals)
- NE (Does not equal)
- GE (Greater than or equal to)
- LE (Less than or equal to)
- GT (Greater than)
- LT (Less than)

Note:

- If you are using a relational operator with the Group of Values list, you must ensure that the operator is appended to the last field in the list, otherwise it will be treated as an additional value for that field.

- To use individual values along with those listed in the Group of Values list, the relational operator must be appended to the last field in the Group of Values list, rather than to the individual field.

String comparisons are performed in lexicographical order. Because the strings are in EBCDIC, the order is lowercase, uppercase, and then numeric. Special character positions depend on the hexadecimal value of the special character itself in relation to the other characters.

Data Set Type

Indicates the type of data sets that should be considered for a match.
Must contain zero or one of the following values:

VSAM|NONVSAM|ALL, where:

VSAM
: VSAM data sets

NONVSAM
: Non-VSAM data sets

All
: Both VSAM and non-VSAM data sets

If nothing is specified, then only VSAM data set types are collected.

Parent topic: IBM Guardium S-TAP for Data Sets administration

CICS collection filtering parameters

Use the following filtering parameters to collect transaction data from CICS®.

CICS User ID

Indicates the CICS logon user ID to use when searching for a match
1 - 8 character CICS logon user ID to match
The user ID can be followed by a comma (,) and a relational operator. If no relational operator is specified, then EQ is assumed.
Wildcards are supported.
If left blank, then activities for all CICS logon user IDs are considered a match

Examples:

CICUSR01
: Matches events that are caused by CICS logon user CICUSR01

CICUSR01,EQ
: Matches events that are caused by CICS logon user CICUSR01

CICUSR%,EQ
: Matches events that are caused by CICS logon users with the prefix CICUSR

CICS Transaction ID

Indicates the CICS transaction ID to use when searching for a match
1 - 4 character CICS transaction ID to match
The transaction ID can be followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Wildcards are supported.
If left blank, then activities for all CICS transaction IDs are considered a match.

Examples:

VTAP
: Matches events that occur within CICS transaction ID VTAP

VTAP,EQ
: Matches events that occur within CICS transaction ID VTAP

VT%,EQ
: Matches events that occur within CICS transaction IDs starting with the prefix VT

CICS Terminal ID

Indicates the CICS terminal ID to use when searching for a match
1 - 4 character CICS terminal ID to match
The terminal ID can be optionally followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Wildcards are supported.
If left blank, then activities for all CICS terminal IDs are considered a match.

Examples

VTAP
: Matches events that occur within CICS transaction ID VTAP

VTAP,EQ
: Matches events that occur within CICS transaction ID VTAP

VT%,EQ
: Matches events that occur within CICS transaction IDs starting with the prefix VT

CICS Region ID

Indicates the CICS region ID to use when searching for a match. The Region ID is defined in the CICS Transaction Server System Initialization Table parameter SYSIDNT.
1 - 4 character CICS region ID to match
The region ID can be followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Wildcards are supported.
If left blank, then activities for all CICS region IDs are considered a match.

Examples:

CICA
: Matches events that occur within the CICS region with an ID of CICA

CICA,EQ
: Matches events that occur within the CICS region with an ID of CICA

CIC%,EQ
: Matches events that occur within the CICS regions with a prefix of CIC

CICS Program Name
: Indicates the CICS program name to use when searching for a match.
1 - 8 character CICS program name to match.
The program name can be followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Wildcards are supported.
If left blank, then activities for all CICS program names are considered a match.

Examples:

PAYROLLA
: Matches events that occur under control of the program that is named PAYROLLA

PAYROLLA,EQ
: Matches events that occur under control of the program that is named PAYROLLA

PAYROLL%,EQ
: Matches events that occur under control of program names that are prefixed with PAYROLL

CICS File ID
: Indicates the CICS file ID to use when searching for a match.
1 - 8 character CICS file ID to match.
The file ID can be followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Wildcards are supported.
If left blank, then activities for all CICS file IDs are considered a match.

Examples:

HRKSDS01
: Matches events that occur for CICS file ID HRKSDS01

HRKSDS01,EQ
: Matches events that occur for CICS file ID HRKSDS01

HRKSDS%,EQ
: Matches events that occur for CICS file IDs prefixed with HRKSDS

CICS Function Code
: Indicates the CICS function code to use when searching for a match. The function code is defined in the CICS Transaction Server Customization Guide. Search for "File control domain exits, XFCFRIN and XFCFROUT." See the description for the XFCFROUT parameter UEP_FC_FUNCTION. The hex values for the UEP_FC_FUNCTION symbolic names are defined in the DFHUEXIT macro in the CICS SDFHMAC macro library.
Two hex characters represent the single character CICS function code.
The function code can be followed by a comma (,) and a relational operator. If no relational operator is provided, then EQ is assumed.
Wildcards are not supported.
If left blank, then all CICS function codes are considered a match.

Examples

01
: Matches events that occur with the CICS function code defined by the hex character 01

01,EQ
: Matches events that occur with the CICS function code defined by the hex character 01

Parent topic: IBM Guardium S-TAP for Data Sets administration

Reference information

This section provides IBM® Guardium® S-TAP® for Data Sets reference information.

- **Simulation mode**
  Simulation mode enables you to simulate agent processing. IBM Guardium S-TAP for Data Sets uses various z/OS MVS system services to gather audit data and move it to the agent address space. The agent address space evaluates this data according to the specified policy, and transmits the audit record to the Guardium appliance by using TCP/IP. To assess the impact on MVS processing, use the STAP_STREAM_EVENTS parameter to simulate data collection.
- **VSAM and non-VSAM data set types and events**
  IBM Guardium S-TAP for Data Sets agent performs data set and record level monitoring for VSAM and non-VSAM data sets. The data set types, as well as the type of events that IBM Guardium S-TAP for Data Sets collects, are described here.
- **SMF record types and contexts**
  SMF records are correlated to IBM Guardium S-TAP for Data Sets contexts, as shown in the following table.
- **Time-to-reporting considerations**
  Learn about the benefits, considerations, and exceptions that apply to the time-to-reporting feature.

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS

Simulation mode

Simulation mode enables you to simulate agent processing. IBM® Guardium® S-TAP® for Data Sets uses various z/OS MVS system services to gather audit data and move it to the agent address space. The agent address space evaluates this data according to the specified policy, and transmits the audit record to the Guardium appliance by

using TCP/IP. To assess the impact on MVS processing, use the STAP_STREAM_EVENTS parameter to simulate data collection.

When STAP_STREAM_EVENTS is set to *N*, the parameter stops the agent TCP/IP data transmission process. The agent performs all data collection processes but does not send the audit record to the Guardium appliance.

The DISPLAY STREAM command display whether the TCP/IP stream of data to the appliance is enabled or disabled. Use this command to verify whether the agent is sending data to the Guardium appliance.

The DIAG command displays the number of created SMF-based records, RLM-based records, and the number of records sent to the appliance. When the agent is in simulation mode (STAP_STREAM_EVENTS=N), the SMF and RLM counters increment with each record created, but the number of records sent to the appliance remains zero. When the agent is not in simulation mode (STAP_STREAM_EVENTS=Y), all counters increment.

Parent topic: Reference information

VSAM and non-VSAM data set types and events

IBM Guardium S-TAP for Data Sets agent performs data set and record level monitoring for VSAM and non-VSAM data sets. The data set types, as well as the type of events that IBM Guardium S-TAP for Data Sets collects, are described here.

Data set level monitoring

The IBM Guardium S-TAP for Data Sets agent collects SMF data for the following data set organizations:

VSAM

ESDS
: Entry sequence data set

KSDS
: Key-sequenced data set

RRDS
: Relative record data set

VRRDS
: Variable length relative record data set

LDS
: Linear data set

Non-VSAM

PS
: Physical sequential

PO
: Partitioned organization

DA
: Direct access

PDSE
: Partitioned organization-extended

The agent audits these data set types by correlating data from a combination of SMF record types to construct one of the following audit events.

VSAM

DATA SET CREATE (DSCR)
: A DEFINE or New Allocation event of a supported data set type

DATA SET OPEN (DSOP)
: An OPEN event against a supported data set type

DATA SET CLOSE (DSCL)
: A CLOSE event against a supported data set type

DATA SET CLOSE INPUT (DSCLI)
: A CLOSE event against a supported data set type that was opened for input

DATA SET CLOSE OUTPUT (DSCLO)
: A CLOSE event against a supported data set type that was opened for output

DATA SET UPDATE (DSUP)
: An UPDATE event against a supported data set type

DATA SET RENAME (DSRN)
: A RENAME event of a supported data set type

DATA SET ALTER (DSALT)
: An ALTER of the attributes of a supported data set type

DATA SET DELETE (DSDL)
: A DELETE event of a supported data set type

Security facility DEFINE violation (DSRDF)
: A security facility DEFINE violation of a supported data set type

Security facility READ violation (DSRRD)
: A security facility READ violation of a supported data set type

Security facility UPDATE violation (DSRUP)
: A security facility UPDATE violation of a supported data set type

Security facility ALTER violation (DSRAL)
: A security facility ALTER violation of a supported data set type

Security facility CONTROL violation (DSRCN)
: A security facility CONTROL violation of a supported data set type

Non-VSAM

DATA SET CREATE (DSCR)
: A DEFINE or New Allocation event of a supported data set type
: For non-SMS data sets, a RENAME event also produces a DATA SET CREATE context record, in addition to a DATA SET RENAME context record.

DATA SET CLOSE (DSCL)
: A CLOSE event against a supported data set type

DATA SET CLOSE INPUT (DSCLI)
: A CLOSE event against a supported data set type that was opened for input

DATA SET CLOSE OUTPUT (DSCLO)
: A CLOSE event against a supported data set type that was opened for output

DATA SET DELETE (DSDL)
: A DELETE event of a supported data set type

DATA SET RENAME (DSRN)
: A RENAME event of a supported data set type

Member add (MADD)
: A member ADD event against a supported data set type

Member replace (MREP)
: A member REPLACE event against a supported data set type

Member rename (MREN)
: A member RENAME event against a supported data set type

Member delete (MDEL)
: A member DELETE event against a supported data set type

STOW initialize (STOWI)
: A STOW initialize event against a supported data set type

Security facility DEFINE violation (DSRDF)
: A security facility DEFINE violation of a supported data set type

Security facility READ violation (DSRRD)
: A security facility READ violation of a supported data set type

Security facility UPDATE violation (DSRUP)
: A security facility UPDATE violation of a supported data set type

Security facility ALTER violation (DSRAL)
: A security facility ALTER violation of a supported data set type

Security facility CONTROL violation (DSRCN)
: A security facility CONTROL violation of a supported data set type

Note: For partitioned organization data sets (PDS and PDSE) that are processed by using EXCP:

- Member additions, updates, and deletions are reported by z/OS® as updates to the base data set.
- IBM Guardium S-TAP for Data Sets reports member additions, updates, and deletions as CLOSE events with an access of OUTPUT.

Record level monitoring

The IBM Guardium S-TAP for Data Sets agent collects record access information for the following VSAM data set types:

KSDS
: Key-sequenced data set

RRDS
: Relative record data set

VRRDS
: Variable length relative record data sets

The agent audits these record level monitoring events:

RECORD INSERT
: A record insert within a data set of a supported type

RECORD DELETE
: A record delete within a data set of a supported type

RECORD READ
: A record read within a data set of a supported type

RECORD UPDATE
: A record update within a data set of a supported type

Parent topic: Reference information

SMF record types and contexts

SMF records are correlated to IBM Guardium S-TAP for Data Sets contexts, as shown in the following table.

Table 1. SMF record types, subtypes, and contexts

Record number	Record subtype	Purpose	SMF context
14		Collecting non-VSAM file activity	CLOSE (non-VSAM input)
15		Collecting non-VSAM file activity	CLOSE (non-VSAM output)
17		Collecting Delete activity	DELETE (non-VSAM)
18		Collecting Rename activity	RENAME (non-VSAM)
30	4, 5	Collecting Job/Step activity	Accounting
42	6	Collecting VSAM type information	Accounting (VSAM)
42	20	Collecting PDS/PDSE member activity	STOW initialization (PDSE directory clearing)
42	21	Collecting PDS/PDSE member activity	DELETE (PDS/PDSE member)
42	24	Collecting PDS/PDSE member activity	ADD/REPLACE (PDS/PDSE member)

Record number	Record subtype	Purpose	SMF context
42	25	Collecting PDS/PDSE member activity	RENAME (PDS/PDSE member)
60*		Collecting VVDS update activity	Data Set ALTER, Data Set CREATE
61*		Collecting DEFINE/CATLG activity	Data Set CREATE
62		Collecting VSAM file activity	OPEN (VSAM)
64		Collecting VSAM I/O statistics	CLOSE (VSAM)
65		Collecting Delete activity	DELETE (VSAM)
66*		Collecting Rename activity	RENAME, ALTER (VSAM)
80		Collecting CICS sign-on security violations	Security Violation

*For more information, see the SMF records section of the *IBM z/OS MVS System Management Facilities (SMF)* documentation, available in the IBM Knowledge Center.

Note:

- There is not a one-to-one correlation between SMF records and context events reported. If more than one SMF record is encountered within a step for a single event, then subsequent records are considered duplicates.
- Audit records for data set events are produced as they occur.
- Data Set CREATE context can appear for RENAME requests of non-SMS, non-VSAM data sets, because the RENAME process generates an SMF type 61 record.

Parent topic: Reference information

Related reference

- Configuring the SMFPRMxx parameter library member

Time-to-reporting considerations

Learn about the benefits, considerations, and exceptions that apply to the time-to-reporting feature.

IBM Guardium S-TAP for Data Sets provides faster real-time reporting for data set level events. When possible, the S-TAP agent immediately delivers data set level information to the Guardium system. The agent presents the data as it occurs, giving you up-to-the-minute results without waiting for jobs to end or SMF type 30 records to be generated.

Benefits

Immediate reporting
: No need to wait for a CICS® address space to terminate, or a TSO user logs off.

Reduced storage usage
: The agent immediately reports data set events to the Guardium system, which substantially reduces the agent storage requirement. The data set event record is complete and ready for transmission to the Guardium system as soon as z/OS® MVS™ creates the source SMF record.

Considerations

Additional event records
: A notable difference as a result of this enhancement is the appearance of data set event records that were not identified in previous versions of this product. Collecting the data set event records in preparation for the SMF type 30 record caused seemingly similar records to merge. For example, a Close event could be reported for a KSDS event, although z/OS DFSMSdfp actually records this as two separate events (one for the Cluster Data component, and one for the Cluster Index component). Improved time-to-reporting now more accurately reflects data set events.

Events Span Data Set Types
: With this feature, and the V10.0 addition of non-VSAM reporting, data set event records might span data set types. For example, when you delete a VSAM KSDS event, z/OS DFSMSdfp deletes a VSAM and a non-VSAM collection of components. Use the DS_TYPE policy filter to adjust this reporting.

Exceptions

To avoid waiting for the SMF type 30 record, the agent scans various z/OS system control blocks in the address space when z/OS is writing the data set SMF record. There are instances when these control blocks are unavailable because of the state of the address space. Before this scan is run, the agent assesses the state of the address space for compatibility. If the address space is not in a compatible state, the agent waits for the SMF type 30 record, which delays reporting of the event until the address space has terminated.

Parent topic: Reference information

Troubleshooting

Use these topics to diagnose and correct problems that you might experience with IBM Guardium S-TAP for Data Sets.

- **Messages and codes**

Parent topic: IBM Security Guardium S-TAP for Data Sets on z/OS

Messages and codes

This information documents the messages and error codes issued by IBM Guardium S-TAP for Data Sets. Messages are presented in ascending alphabetical and numerical order.

- **Error message code descriptions**

Parent topic: Troubleshooting

Error message code descriptions

IBM Guardium S-TAP for Data Sets error messages adhere to the following format: AUV*nnnx*

Where:

AUV
: Indicates that the message was issued by IBM Guardium S-TAP for Data Sets.

nnn
: Indicates the message identification number.

x
: Indicates the severity of the message:

Table 1. Error message severity codes

Severity Code	Description
A	Indicates that operator intervention is required before processing can continue.
E	Indicates that an error occurred, which might or might not require operator intervention.
I	Indicates that the message is informational only.
W	Indicates that the message is a warning to alert you to a possible error condition.

- **AUV1001I**
  RULEDEFS ACTIVATION SUCCESSFUL –*ssss*
- **AUV1002E**
  INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING
- **AUV1003E**
  INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING
- **AUV1004E**
  UNABLE TO LOCATE REQUIRED DDNAME - CONTROL
- **AUV1005E**
  ERROR OCCURRED DURING SWAREQ PROCESSING FOR JFCB FOR DDNAME CONTROL, RC=*rrrrrrrr*
- **AUV1006E**
  UNABLE TO LOCATE REQUIRED DDNAME - OPTIONS
- **AUV1007E**
  ERROR OCCURRED DURING SWAREQ PROCESSING FOR JFCB FOR DDNAME OPTIONS, RC=*rrrrrrrr*
- **AUV1008I**
  RULEDEFS NOT ACTIVATED –*ssss*
- **AUV1009E**
  OPEN FAILED FOR PROCESSING OPTIONS MEMBER; DEFAULT OPTIONS USED
- **AUV1012E**
  ATTACH FOR AUVMAIN FAILED, RC=*rrrrrrrr*
- **AUV1013I**
  PRODUCT TERMINATION IS COMPLETE
- **AUV1014E**
  INVALID START PARAMETERS SPECIFIED; IGNORED
- **AUV1015E**
  INVALID PARM SPECIFIED - *parm*
- **AUV1016E**
  DELIMITER "=" IS MISSING - *parm*
- **AUV1017I**
  START PARAMETER SPECIFIED - *parm*
- **AUV1018E**
  INVALID VALUE SPECIFIED FOR PARAMETER - *parm*
- **AUV1019I**
  START PARAMETER SPECIFIED - *parm*
- **AUV1020E**
  VALUE SPECIFIED FOR PARAMETER - *parm*
- **AUV1021E**
  INVALID OPTION SPECIFIED - *pppppppp*
- **AUV1022E**
  INVALID KEYWORD/DELIMITER - *pppppppp*
- **AUV1023E**
  INVALID VALUE SPECIFIED FOR OPTION - *pppppppp*
- **AUV1024I**
  PROCESSING OPTION SET - SUBSYS=*ssss*
- **AUV1025E**
  INVALID VALUE SPECIFIED FOR OPTION - SUBSYS=*ssss*
- **AUV1026I**
  PROCESSING OPTION SET - INITIAL_RULEDEF=*rrrrrrrr*
- **AUV1027E**
  INVALID VALUE SPECIFIED FOR OPTION -INITIAL_RULEDEF=*rrrrrrrr*
- **AUV1028I**
  PROCESSING OPTION SET - PORT=*nnnnn*
- **AUV1029E**
  INVALID VALUE SPECIFIED FOR OPTION - PORT=*nnnnn*
- **AUV1030I**
  PROCESSING OPTION SET – APPLIANCE_PING_RATE=*nnnnn*
- **AUV1031E**
  INVALID VALUE SPECIFIED FOR OPTION – APPLIANCE_PING_RATE=*nnnnn*

- **AUV1032I**
  PROCESSING OPTION SET – APPLIANCE_RETRY_INTERVAL=*nnnnn*
- **AUV1033E**
  VALUE SPECIFIED FOR OPTION – APPLIANCE_RETRY_INTERVAL=*nnnnn*
- **AUV1034E**
  ERROR IN NAME/TOKEN RETRIEVAL PROCESSING, RC=*rrrrrrrr*
- **AUV1035E**
  NAME/TOKEN ALREADY EXISTS, BUT TOKEN IS ZERO
- **AUV1036E**
  NAME/TOKEN ALREADY EXISTS, BUT TOKEN DOES NOT POINT TO A VALID PRODUCT BLOCK
- **AUV1038E**
  UNABLE TO OBTAIN STORAGE FOR PRODUCT CONTROL BLOCK, RC=*rrrrrrrr*
- **AUV1040E**
  ERROR IN NAME/TOKEN CREATE PROCESSING, RC=*rrrrrrrr*
- **AUV1041I**
  PRODUCT INTERCEPTS HAVE BEEN ESTABLISHED
- **AUV1042E**
  UNABLE TO OBTAIN STORAGE FOR COMMON AREA ROUTINE, RC=*rrrrrrrr*
- **AUV1043E**
  BLDL FAILED FOR *mmmmmmmm*, RC=*rrrrrrrr*
- **AUV1044E**
  UNABLE TO DETERMINE ORIGIN OF *mmmmmmmm*
- **AUV1046E**
  PRIVATE LOAD FAILED FOR *mmmmmmmm*
- **AUV1047E**
  COMMON LOAD FAILED FOR *mmmmmmmm*
- **AUV1048I**
  PROCESSING OPTION SET: APPLIANCE_CONNECT_RETRY_COUNT
- **AUV1049E**
  INVALID VALUE SPECIFIED FOR OPTION – APPLIANCE_CONNECT_RETRY_COUNT=*nnnnn*
- **AUV1050E**
  UNABLE TO ESTABLISH *NNNNNNNNNNNNNNNN* EXIT, RC=*RRRRRRRR*, RS=*SSSSSSSS*
- **AUV1052E**
  UNABLE TO DELETE *NNNNNNNNNNNNNNNN* EXIT, RC=*RRRRRRRR*, RS=*SSSSSSSS*
- **AUV1054E**
  GSSB IS NOT PRESENT
- **AUV1055E**
  GSSB CONTROL BLOCK ID IS INVALID
- **AUV1056I**
  PROCESSING OPTION SET – APPLIANCE_NETWORK_REQUEST_TIMEOUT=*nnnnn*
- **AUV1058E**
  UNABLE TO LOCATE LPDE FOR IGC0005E
- **AUV1058I**
  PROCESSING OPTION SET – APPLIANCE_SERVER=*a**
- **AUV1059E**
  INVALID VALUE SPECIFIED FOR OPTION - APPLIANCE_SERVER=*a**
- **AUV1060I**
  PROCESSING OPTION SET – AUDIT=*a**
- **AUV1061E**
  VALUE SPECIFIED FOR OPTION – AUDIT=*a**
- **AUV1062I**
  PROCESSING OPTION SET – CICS_SUPPORT=*nnnnnnn*
- **AUV1063E**
  INVALID VALUE SPECIFIED FOR OPTION – CICS_SUPPORT=*nnnnnnn*
- **AUV1064W**
  Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.
- **AUV1065E**
  UNABLE TO LOCATE LPDE FOR IDA0192A
- **AUV1066E**
  UNABLE TO LOCATE IDA0192A
- **AUV1067E**
  PAGE SERVICE LIST EXHAUSTED FOR *xx* INTERCEPT
- **AUV1068E**
  UNABLE TO OBTAIN STORAGE FOR *xx* INTERCEPT, RC=*rrrrrrrr*
- **AUV1069E**
  UNABLE TO LOCATE IDA0200T
- **AUV1070I**
  TCP/IP STREAMING DISABLED DUE TO USER SETTING
- **AUV1073W**
  MAXIMUM ACTIVE SUBSYSTEMS EXCEEDED (1)
- **AUV1074E**
  DUPLICATE SUBSYSTEM FOUND FOR SSID=*ssss*
- **AUV1077I**
  PII DATA NOT BEING TRANSMITTED DUE TO USER SETTING
- **AUV1080E**
  ERROR IN NAME/TOKEN DELETE PROCESSING, RC=*rrrrrrrr*
- **AUV1081E**
  GETMAIN FAILED FOR JSPB VECTOR TABLE, RC=*rrrrrrrr*
- **AUV1082W**
  IEFU86 EXIT IS NOT DEFINED

- **AUV1100E**
  ACRONYM CHECK FAILED FOR GSSB
- **AUV1101E**
  INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING
- **AUV1102E**
  ERROR OCCURRED IN CROSS-MEMORY INITIALIZATION
- **AUV1103E**
  ATTACH FOR AUVPING FAILED, RC=*rrrrrrrr -ssss*
- **AUV1105E**
  ATTACH FOR AUVSSRP FAILED, RC=*rrrrrrrr -ssss*
- **AUV1105I**
  SUBSYSTEM IS ACTIVE AND ENABLED
- **AUV1106I**
  SUBSYSTEM INITIALIZATION IS COMPLETE
- **AUV1107I**
  PRODUCT TERMINATION HAS BEEN REQUESTED
- **AUV1111E**
  UNABLE TO OBTAIN STORAGE FOR COMMON AREA ROUTINE, RC=*rrrrrrrr*
- **AUV1112E**
  BLDL FAILED FOR *mmmmmmmm*, RC=*rrrrrrrr*
- **AUV1113E**
  UNABLE TO DETERMINE ORIGIN OF *mmmmmmmm*
- **AUV1115E**
  INITIAL LOAD FAILED FOR *mmmmmmmm*
- **AUV1116E**
  DIRECTED LOAD FAILED FOR *mmmmmmmm*
- **AUV1117E**
  NON-ZERO RETURN CODE FROM SYSEVENT, RC=*rrrrrrrr -ssss*
- **AUV1122E**
  INVALID COMMAND SPECIFIED - *cccccccc -ssss*
- **AUV1123E**
  INVALID COMMAND SPECIFIED - *cccccccc -ssss*
- **AUV1123W**
  ACTIVE SUBSYSTEM DETECTED; PRODUCT-LEVEL MODULE NOT RE-INITIALIZED
- **AUV1124E**
  EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*
- **AUV1125E**
  INSUFFICIENT OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*
- **AUV1126E**
  INVALID OPERAND SPECIFIED FOR COMMAND - *cccccccc -ssss*
- **AUV1127I**
  SUBSYSTEM IS ACTIVE | INACTIVE AND ENABLED | DISABLED *-ssss*
- **AUV1128E**
  INVALID COMMAND SPECIFIED - *command*
- **AUV1129I**
  THERE ARE CURRENTLY NO SUBSYSTEMS *-ssss*
- **AUV1130I**
  SUBSYSTEM xxxx IS ACTIVE | INACTIVE AND ENABLED | DISABLED *-ssss*
- **AUV1131I**
  RULEDEFS ACTIVATED ON *mm/dd/yyyy* AT *hh:mm:ss* FROM MEMBER *mmmmmmmm -ssss*
- **AUV1132I**
  RULEDEFS NOT ACTIVATED *-ssss*
- **AUV1136I**
  PRODUCT-LEVEL TRACING IS ENABLED | DISABLED *-ssss*
- **AUV1137I**
  SUBSYSTEM-LEVEL TRACING IS ENABLED | DISABLED *-ssss*
- **AUV1138E**
  EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*
- **AUV1140I**
  SMF MONITORING SUCCESSFULLY ENABLED – *SSSS*
- **AUV1141I**
  SUBSYSTEM IS NOW ENABLED *-ssss*
- **AUV1142I**
  TCP/IP STREAM SUCCESSFULLY ENABLED *-ssss*
- **AUV1143I**
  SMF MONITORING SUCCESSFULLY DISABLED –*SSSS*
- **AUV1144I**
  TRACING FOR PRODUCT IS NOW ENABLED *-ssss*
- **AUV1145I**
  TRACING FOR SUBSYSTEM IS NOW ENABLED *-ssss*
- **AUV1146E**
  EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*
- **AUV1147I**
  TCP/IP STREAM IS *EEEEEEEE -ssss*
- **AUV1149I**
  SUBSYSTEM IS NOW DISABLED *-ssss*
- **AUV1150I**
  TCP/IP STREAM SUCCESSFULLY DISABLED *-ssss*
- **AUV1151E**
  SMF MONITORING DISABLE NOT SUCCESSFUL –*SSSS*

- **AUV1152I**
  TRACING FOR PRODUCT IS NOW DISABLED -*ssss*
- **AUV1153I**
  TRACING FOR SUBSYSTEM IS NOW DISABLED -*ssss*
- **AUV1154E**
  EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc* -*ssss*
- **AUV1155E**
  SMF MONITORING ENABLE FAILED –*SSSS*
- **AUV1156E**
  SMF MONITORING ALREADY ENABLED –*SSSS*
- **AUV1157E**
  OPERANDS SPECIFIED FOR COMMAND - *command*
- **AUV1158E**
  SMF MONITORING ALREADY DISABLED –*SSSS*
- **AUV1175I**
  DDDDDDDD MEMBER ACTIVATION SUCCESSFUL –*SSSS*
- **AUV1176E**
  DDDDDDDD MEMBER ACTIVATION FAILED – SEE JESYSMSG FOR DETAILS –*SSSS*
- **AUV1176I**
  dddddddd MEMBER *mmmmmmmm* ACTIVATION FAILED - SEE JESYSMSG FOR DETAILS -*ssss*
- **AUV1177I**
  dddddddd MEMBER *mmmmmmmm* ACTIVATION FAILED - FAILURE CODE *cccc* -*ssss*
- **AUV1179E**
  DDDDDDDD MEMBER ACTIVATION FAILED - FAILURE CODE *CCCCCCCC* –*SSSS*
- **AUV1184E**
  COMMAND VERB NOT UNIQUE - cccccccc -ssss
- **AUV1185E**
  INVALID COMMAND SYNTAX SPECIFIED - *ssss*
- **AUV1191E**
  INVALID MODULE NAME SPECIFIED - *cccccccc*
- **AUV1192I**
  MODULE *mmmmmmmm vvvv ffffffff dddddddd ttttt*
- **AUV1193I**
  MODULE *mmmmmmmm* LOCATED AT *aaaaaaaa* (*stgloc*)
- **AUV1195E**
  ERROR OCCURRED DURING FREEMAIN FOR GPB, RC=*rrrrrrrr*
- **AUV1196E**
  UNEXPECTED VCON COUNT FOR *xx* INTERCEPT; EXPECTED=*eee*, FOUND=*fff*
- **AUV1200E**
  UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA
- **AUV1202E**
  UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA
- **AUV1203E**
  UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA
- **AUV1204E**
  UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA
- **AUV1213E**
  ERROR RETRIEVING SSRE
- **AUV1214E**
  UNEXPECTED SSRE QUEUE ERROR
- **AUV1215E**
  UNEXPECTED SSRE QUEUE ERROR
- **AUV1400I**
  RECORD LEVEL MONITORING IS *EEEEEEEE* -*SSSS*
- **AUV1401I**
  RECORD LEVEL MONITORING INTERCEPTS ARE *EEEEEEEE* -*SSSS*
- **AUV1402I**
  CURRENT POLICY *EEE* -*SSSS*
- **AUV1405I**
  RECORD LEVEL MONITORING SUCCESSFULLY ENABLED -*SSSS*
- **AUV1406W**
  RECORD LEVEL MONITORING SUCCESSFULLY ENABLED, BUT NO RLM FILTERS EXIST IN CURRENT POLICY -*SSSS*
- **AUV1408W**
  POLICY CONTAINING RECORD LEVEL MONITORING FILTERS ACTIVATED, BUT RLM IS CURRENTLY DISABLED -*SSSS*
- **AUV1410I**
  PROCESSING OPTION SET - SOCKET_CONNECT_TIMEOUT=*nnnnn*
- **AUV1411E**
  INVALID VALUE SPECIFIED FOR OPTION - SOCKET_CONNECT_TIMEOUT=*nnnnn*
- **AUV1412I**
  PROCESSING OPTION SET - OUTAGE_SPILLAREA_SIZE=*nnnnnnn*
- **AUV1413E**
  INVALID VALUE SPECIFIED FOR OPTION – OUTAGE_SPILLAREA_SIZE=*nnnnnnn*
- **AUV1414I**
  PROCESSING OPTION SET - INTERNAL_BUFFER_SIZE=*nnnnnnn*
- **AUV1415E**
  INVALID VALUE SPECIFIED FOR OPTION INTERNAL_BUFFER_SIZE=*nnnnnnn*
- **AUV1416I**
  PROCESSING OPTION SET - APPLIANCE_SERVER_FAILOVER=a*
- **AUV1417E**
  INVALID VALUE SPECIFIED FOR OPTION - *keyword*=a*

- **AUV1418I**
  PROCESSING OPTION SET - IAM_SMF_RECORD_ID = *nnn*
- **AUV1419E**
  INVALID VALUE SPECIFIED FOR OPTION - IAM_SMF_RECORD_ID = *nnn*
- **AUV1420I**
  PROCESSING OPTION SET - ACF_SMF_RECORD_ID = *nnn*
- **AUV1421E**
  INVALID VALUE SPECIFIED FOR OPTION - ACF_SMF_RECORD_ID = *nnn*
- **AUV1422I**
  PROCESSING OPTION SET - APPLIANCE_SERVER_LIST(*nnn*)
- **AUV1423E**
  INVALID VALUE SPECIFIED FOR OPTION - APPLIANCE_SERVER_LIST(*nnn*)
- **AUV1424I**
  PROCESSING OPTION SET - MEGABUFFER_COUNT =*nnnnnnn*
- **AUV1425E**
  INVALID VALUE SPECIFIED FOR OPTION MEGABUFFER_COUNT =*nnnnnnn*
- **AUV1438I**
  SMF MONITORING IS *EEEEEEEE -SSSS*
- **AUV1439I**
  SMF MONITORING EXITS ARE *EEE -SSSS*
- **AUV1450W**
  SMF RECORDING TEST FAILED, RC=*cc*, TYPE=*nnnn*, SUBSYSTEM=*ssss*
- **AUV1747E**
  SUBSYSTEM IS NOT ACTIVE OR ENABLED
- **AUV1748W**
  POLICY CONTAINING RECORD LEVEL MONITORING FILTERS ACTIVATED, BUT RLM IS CURRENTLY DISABLED -*SSSS*
- **AUV2000E**
  INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING
- **AUV2030E**
  UNRECOGNIZED INTERCEPT ID ENCOUNTERED (*XX*)
- **AUV2040E**
  ERROR OCCURRED DURING SWAREQ PROCESSING FOR JCT, RC=*rrrrrrrr*
- **AUV2041E**
  ERROR OCCURRED DURING SWAREQ PROCESSING FOR SCT, RC=*rrrrrrrr*
- **AUV2042E**
  ERROR OCCURRED DURING SWAREQ PROCESSING FOR JMR, RC=*rrrrrrrr*
- **AUV2097I**
  JCT UNAVAILABLE FOR JSPB LOOK-UP FOR ASID *xxxx*
- **AUV2098I**
  ASID *xxxx* EXCEEDS GJVT MAX; ASVTMAXU=*xxxxxxxx*
- **AUV2104E**
  ERROR OCCURRED IN FREEMAIN OF AUVSMFX1, RC=*RRRRRRRR*
- **AUV2170I**
  ATTEMPTING TO CONNECT TO THE GUARDIUM APPLIANCE
- **AUV2171I**
  CALL TO GUARDIUM APPLIANCE SUCCESSFUL
- **AUV2172E**
  function CALL TO GUARDIUM APPLIANCE FAILED
- **AUV2173E**
  function CALL TO GUARDIUM APPLIANCE FAILED, RC = *rc* RC_STP= *rc* RS_STP= *rs* RC_GDM= *rc* RC_PB = *rc* RC_LST= *rc* RS_LST= *rs*
- **AUV2174E**
  SPILL FILE FULL, DATA LOSS MIGHT OCCUR
- **AUV2175E**
  CONNECTION LOST WITH NO SPILL FILE, DATA LOSS MIGHT OCCUR
- **AUV2176E**
  UNABLE TO OBTAIN STORAGE, DATA LOSS MIGHT OCCUR
- **AUV2177E**
  RULEDEF NOT ACTIVATED - CHECK SYSPRINT FOR REASON
- **AUV2178I**
  SPILL FILE IS *xx*% FULL
- **AUV2179E**
  UNABLE TO OBTAIN REQUESTED STORAGE FOR INTERNAL_BUFFER_SIZE: dddd. PROCESSING CONTINUES.
- **AUV2180W**
  WRITING TO SPILL FILE
- **AUV2181I**
  NO LONGER WRITING TO SPILL FILE
- **AUV2182I**
  CONNECTION ESTABLISHED TO *x*
- **AUV2183W**
  STORAGE SHORTAGE DETECTED; ONE OR MORE EVENTS NOT RECORDED
- **AUV2184W**
  STORAGE SHORTAGE RELIEVED; EVENT RECORDING RESUMED. EVENTS LOST=????????
- **AUV2185I**
  UNEXPECTED PRODUCT STATE DETECTED. ATTEMPTING RESTART.
- **AUV2186E**
  UNABLE TO RESOLVE HOST NAME *a**
- **AUV2900E**
  INVALID STORAGE REQUEST FOR CONTROL BLOCK *nnnn -ssss*
- **AUV2901E**
  INSUFFICIENT VIRTUAL STORAGE FOR CONTROL BLOCK *nnnn -ssss*

- **AUV2902E**
  ACRONYM CHECK FAILED WHILE ATTEMPTING TO FREE *nnnn*, DATA=*dddd -ssss*
- **AUV2903E**
  FAILURE OCCURRED DURING FREEMAIN FOR *nnnn -ssss*
- **AUV3000E**
  ERROR ENABLING AUVFROUT: EIBRCODE=*NNNNNNNNNNN*
- **AUV3001E**
  ERROR OBTAINING GWA ADDR: EIBRCODE=*NNNNNNNNNNN*
- **AUV3003E**
  ERROR STARTING AUVFROUT: EIBRCODE=*NNNNNNNNNNN*
- **AUV3004I**
  AUVPLTPI XFCFROUT GLOBAL USER EXIT SUCCESSFULLY ENABLED AND STARTED
- **AUV3005E**
  ERROR STOPPING AUVFROUT: EIBRCODE=*NNNNNNNNNNN*
- **AUV3006E**
  ERROR OBTAINING GWA ADDR: EIBRCODE=*NNNNNNNNNNN*
- **AUV3008E**
  ERROR DISABLING AUVFROUT: EIBRCODE=*NNNNNNNNNNN*
- **AUV3009I**
  AUVPLTPS XFCFROUT GLOBAL USER EXIT SUCCESSFULLY STOPPED AND DISABLED
- **AUV3010W**
  CICS PLTPI INSTALLED BUT CICS_SUPPORT NOT SPECIFIED IN OPTIONS

Parent topic: Messages and codes

AUV1001I RULEDEFS ACTIVATION SUCCESSFUL –*ssss*

Explanation

This message is issued to the operator console following successful activation of rule definitions using the ACTIVATE RULEDEFS operator command.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1002E INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING

Explanation

Product initialization was unable to obtain the required above-the-line storage.

User response

Increase the amount of available above-the-line storage and attempt to restart the product. If this is not successful, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1003E INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING

Explanation

Product initialization was unable to obtain the required below-the-line storage.

User response

Increase the amount of available below-the-line storage and attempt to restart the product. If this is not successful, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1004E UNABLE TO LOCATE REQUIRED DDNAME - CONTROL

Explanation

During product initialization, the CONTROL DD statement was unable to be located in the product started task procedure.

User response

The CONTROL DD statement is required. Add the CONTROL DD statement to the product started task procedure and retry.
Parent topic: Error message code descriptions

AUV1005E ERROR OCCURRED DURING SWAREQ PROCESSING FOR JFCB FOR DDNAME CONTROL, RC=*rrrrrrrr*

Explanation

An internal error (*rrrrrrrr*) occurred while processing the CONTROL DD statement during product initialization.

User response

Make sure that the CONTROL DD statement points to a valid partitioned data set and retry. If the error persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1006E UNABLE TO LOCATE REQUIRED DDNAME - OPTIONS

Explanation

During product initialization, the OPTIONS DD statement was unable to be located in the product started task procedure.

User response

The OPTIONS DD statement is required. Add the OPTIONS DD statement to the product started task procedure and retry.
Parent topic: Error message code descriptions

AUV1007E ERROR OCCURRED DURING SWAREQ PROCESSING FOR JFCB FOR DDNAME OPTIONS, RC=*rrrrrrrr*

Explanation

An internal error (*rrrrrrrr*) occurred while processing the OPTIONS DD statement during product initialization.

User response

Make sure that the OPTIONS DD statement points to a valid data set and retry. If the error persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1008I RULEDEFS NOT ACTIVATED –*ssss*

Explanation

This message is issued in response to the DISPLAY RULEDEFS operator command when no rule definitions have been activated.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1009E OPEN FAILED FOR PROCESSING OPTIONS MEMBER; DEFAULT OPTIONS USED

Explanation

Open processing was unsuccessful for the OPTIONS member so the default options were used.

User response

Make sure that the OPTIONS DD statement points to a valid data set and retry. If the error continues, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1012E ATTACH FOR AUVMAIN FAILED, RC=*rrrrrrrr*

Explanation

During product initialization, the startup of an internal task failed. The value *rrrrrrrr* identifies the internal error code.

User response

Examine other error messages that might have occurred at the same time as this message to aid in determining the cause of the failure. If no cause can be determined, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1013I PRODUCT TERMINATION IS COMPLETE

Explanation

This message is issued in response to the product shutdown command at completion of termination processing.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1014E INVALID START PARAMETERS SPECIFIED; IGNORED

Explanation

An invalidly constructed parameter was specified on the START command for the started task; it will be ignored.

User response

Correct the START command parameter and restart the started task.
Parent topic: Error message code descriptions

AUV1015E INVALID PARM SPECIFIED - *parm*

Explanation

An unrecognized parameter was specified on the START command for the started task where parm is the unrecognized parameter.

User response

Correct the START command parameter and restart the started task.
Parent topic: Error message code descriptions

AUV1016E DELIMITER "=" IS MISSING - *parm*

Explanation

The START parameter specified by parm requires an equal sign followed by a keyword value; no equal sign was found.

User response

Correct the START command parameter and restart the started task.
Parent topic: Error message code descriptions

AUV1017I START PARAMETER SPECIFIED - *parm*

Explanation

The TRACING START parameter specified by parm was successfully recognized and processed.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1018E INVALID VALUE SPECIFIED FOR PARAMETER - *parm*

Explanation

The TRACING START parameter keyword value for the parameter specified by *parm* was invalid.

User response

Correct the START parameter keyword value and restart the started task.
Parent topic: Error message code descriptions

AUV1019I START PARAMETER SPECIFIED - *parm*

Explanation

The KEY START parameter specified by parm was successfully recognized and processed.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1020E VALUE SPECIFIED FOR PARAMETER - *parm*

Explanation

The KEY START parameter keyword value for the parameter specified by parm was invalid.

User response

Correct the START parameter keyword value and restart the started task.
Parent topic: Error message code descriptions

AUV1021E INVALID OPTION SPECIFIED - *pppppppp*

Explanation

During product initialization, an invalid keyword was encountered when processing the subsystem options in the OPTIONS member. The value *pppppppp* is the invalid option encountered — or the value "(NONE)" if blank options were specified.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1022E INVALID KEYWORD/DELIMITER - *pppppppp*

Explanation

During product installation, while processing the subsystem options in the OPTIONS member, an invalid keyword or delimiter was encountered. The value *pppppppp* indicates the associated keyword.

User response

Correct the specified option keyword or delimiter and restart the product.
Parent topic: Error message code descriptions

AUV1023E INVALID VALUE SPECIFIED FOR OPTION - *pppppppp*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, a keyword was encountered with an invalid value. The value *pppppppp* indicates the option with the incorrect value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1024I PROCESSING OPTION SET - SUBSYS=*ssss*

Explanation

This message is issued during product initialization to display the value (*ssss*) set for the SUBSYS keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1025E INVALID VALUE SPECIFIED FOR OPTION - SUBSYS=*ssss*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the SUBSYS option. The value *ssss* indicates the invalid value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1026I PROCESSING OPTION SET - INITIAL_RULEDEF=*rrrrrrrr*

Explanation

This message is issued during product initialization to display the value (*rrrrrrrr*) specified for the INITIAL_RULEDEF keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1027E INVALID VALUE SPECIFIED FOR OPTION -INITIAL_RULEDEF=*rrrrrrrr*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the INITIAL_RULEDEF option. The value *rrrrrrrr* indicates the invalid value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1028I PROCESSING OPTION SET - PORT=*nnnnn*

Explanation

This message is issued during product initialization to display the value (*nnnnn*) specified for the PORT keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1029E INVALID VALUE SPECIFIED FOR OPTION - PORT=*nnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the PORT option. The value *nnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1030I PROCESSING OPTION SET – APPLIANCE_PING_RATE=*nnnnn*

Explanation

This message is issued during product initialization to display the value (*nnnnn*) specified for the APPLIANCE_PING_RATE keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1031E INVALID VALUE SPECIFIED FOR OPTION – APPLIANCE_PING_RATE=*nnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the APPLIANCE_PING_RATE option. The value *nnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart the product.

Parent topic: Error message code descriptions

AUV1032I PROCESSING OPTION SET – APPLIANCE_RETRY_INTERVAL=*nnnnn*

Explanation

This message is issued during product initialization to display the value (*nnnnn*) specified for the APPLIANCE_RETRY_INTERVAL keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1033E VALUE SPECIFIED FOR OPTION – APPLIANCE_RETRY_INTERVAL=*nnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the APPLIANCE_RETRY_INTERVAL option. The value *nnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1034E ERROR IN NAME/TOKEN RETRIEVAL PROCESSING, RC=*rrrrrrrr*

Explanation

During product initialization, an internal system error (*rrrrrrrr*) was encountered in establishing the product.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1035E NAME/TOKEN ALREADY EXISTS, BUT TOKEN IS ZERO

Explanation

During product initialization, an internal system error was encountered in establishing the product.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1036E NAME/TOKEN ALREADY EXISTS, BUT TOKEN DOES NOT POINT TO A VALID PRODUCT BLOCK

User response

IPL the system before starting the product. If this does not resolve the problem, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1038E UNABLE TO OBTAIN STORAGE FOR PRODUCT CONTROL BLOCK, RC=*rrrrrrrr*

Explanation

During product initialization, above-the-line CSA storage was unable to be obtained a product control block as indicated by the internal return code *rrrrrrrr*.

User response

Investigate and correct the shortage of above-the-line CSA storage and restart the product. If the problem persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1040E ERROR IN NAME/TOKEN CREATE PROCESSING, RC=*rrrrrrrr*

Explanation

During product initialization, an internal system error (*rrrrrrrr*) was encountered in establishing the product.

User response

Please contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1041I PRODUCT INTERCEPTS HAVE BEEN ESTABLISHED

Explanation

This message is issued when all intercepts have been successfully established.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1042E UNABLE TO OBTAIN STORAGE FOR COMMON AREA ROUTINE, RC=*rrrrrrrr*

Explanation

During product initialization, above-the-line CSA storage was unable to be obtained for loading a required product routine as detailed by the internal return code *rrrrrrrr*.

User response

Investigate and correct the shortage of above-the-line CSA storage and restart the product. If the problem persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1043E BLDL FAILED FOR *mmmmmmmm*, RC=*rrrrrrrr*

Explanation

During product initialization, a required load module was unable to be successfully located. The value *mmmmmmmm* identifies the load module and the value *rrrrrrrr* specifies the internal return code in error.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task, or in the system LINKLIST concatenation and then restart the product.
Parent topic: Error message code descriptions

AUV1044E UNABLE TO DETERMINE ORIGIN OF *mmmmmmmm*

Explanation

During product initialization while processing the product load module *mmmmmmmm* an error was encountered.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task or in the system LINKLIST concatenation and restart the product.
Parent topic: Error message code descriptions

AUV1046E PRIVATE LOAD FAILED FOR *mmmmmmmm*

Explanation

During product initialization, the processing of a product load module *(mmmmmmm*) to be located in above-the-line private storage failed.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task, or in the system LINKLIST concatenation and then restart the product. In addition, check the available amount of above-the-line private storage available for the product started task. After correcting the problem, restart the product. If the error cannot be determined, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1047E COMMON LOAD FAILED FOR *mmmmmmmm*

Explanation

During product initialization, the processing of a product load module (*mmmmmmm*) to be located in above-the-line common storage, failed.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task, or in the system LINKLIST concatenation and then restart the product. In addition, check the available amount of above-the-line common storage available for the product started task. After correcting the problem, restart the product. If the error cannot be determined, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1048I PROCESSING OPTION SET: APPLIANCE_CONNECT_RETRY_COUNT

Explanation

This message is issued during product initialization to display the value set (*nnnnn*) specified for the APPLIANCE_CONNECT_RETRY_COUNT keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1049E INVALID VALUE SPECIFIED FOR OPTION – APPLIANCE_CONNECT_RETRY_COUNT=*nnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the APPLIANCE_CONNECT_RETRY_COUNT option. The value *nnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1050E UNABLE TO ESTABLISH *NNNNNNNNNNNNNNN* EXIT, RC=*RRRRRRRR*, RS=*SSSSSSSS*

Explanation

During started task initialization or as a result of the ENABLE SMFEXIT1 operator command, an error was encountered attempting to establish the SMF exit named *NNNNNNNNNNNNNNN*. The return code encountered is specified by *RRRRRRRR* and the reason code is specified by *SSSSSSSS*.

This message might be caused by having more than one agent active on a single z/OS image. Only one agent per z/OS image is required.

User response

Verify that no more than one agent is active per z/OS image. If that does not resolve the error, contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1052E UNABLE TO DELETE *NNNNNNNNNNNNNNN* EXIT, RC=*RRRRRRRR*, RS=*SSSSSSSS*

Explanation

During started task termination or as a result of the DISABLE SMFEXIT1 operator command, an error was encountered attempting to delete the SMF exit named *NNNNNNNNNNNNNNN*. The return code encountered is specified by *RRRRRRRR* and the reason code is specified by *SSSSSSSS*.

User response

Contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1054E GSSB IS NOT PRESENT

Explanation

During activation of a policy RULEDEFS member, a necessary Security Guardium® S-TAP® for Data Sets control block could not be located.

User response

Ensure that the Security Guardium S-TAP for Data Sets started task has been successfully started. If no error was encountered during the initialization of the started task, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1055E GSSB CONTROL BLOCK ID IS INVALID

Explanation

During activation of a policy RULEDEFS member, a necessary Security Guardium® S-TAP® for Data Sets control block was located but it is not valid.

User response

Ensure that the Security Guardium S-TAP for Data Sets started task has been successfully started. If no error was encountered during the initialization of the started task, contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1056I PROCESSING OPTION SET – APPLIANCE_NETWORK_REQUEST_TIMEOUT=*nnnnn*

Explanation

This message is issued during product initialization to display the value (*nnnnn*) that is specified for the APPLIANCE_NETWORK_REQUEST_TIMEOUT keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1058E UNABLE TO LOCATE LPDE FOR IGC0005E

Explanation

During product initialization, a required pointer to an operating system module could not be located.

User response

Contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1058I PROCESSING OPTION SET – APPLIANCE_SERVER=*a**

Explanation

This message is issued during product initialization to display the value (*a**) specified for the APPLIANCE_SERVER keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1059E INVALID VALUE SPECIFIED FOR OPTION - APPLIANCE_SERVER=*a**

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the APPLIANCE_SERVER option. The value *a** indicates the invalid value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1060I PROCESSING OPTION SET – AUDIT=*a**

Explanation

This message is issued during product initialization to display the value (*a**) specified for the AUDIT keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1061E VALUE SPECIFIED FOR OPTION – AUDIT=*a**

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the AUDIT option. The value *a** indicates the invalid value.

User response

Correct the specified option keyword and restart the product.
Parent topic: Error message code descriptions

AUV1062I PROCESSING OPTION SET – CICS_SUPPORT=*nnnnnnn*

Explanation

This message is issued during product initialization to display the value *nnnnnnn* that was specified for the CICS_SUPPORT keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1063E INVALID VALUE SPECIFIED FOR OPTION – CICS_SUPPORT=*nnnnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the CICS_SUPPORT option. The value *nnnnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart the product.

Parent topic: Error message code descriptions

AUV1064W Invalid port specified for APPLIANCE_PORT. Port 16022 will be used instead.

Explanation

The APPLIANCE_PORT parameter currently supports a setting of 16022 or 16023. If APPLIANCE_PORT is specified with a value other than 16022 or 16023, message AUV1064W is issued and port 16022 is used instead.

User response

Change the APPLIANCE_PORT parameter setting to one of the supported values, or remove the parameter.
Parent topic: Error message code descriptions

AUV1065E UNABLE TO LOCATE LPDE FOR IDA0192A

Explanation

During Record level monitoring initialization, a required pointer to an operating system module could not be located.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1066E UNABLE TO LOCATE IDA0192A

Explanation

During Record level monitoring initialization, a required operating system module could not be located.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1067E PAGE SERVICE LIST EXHAUSTED FOR *xx* INTERCEPT

Explanation

During Record level monitoring initialization, an unexpected internal error occurred during an attempt to establish a product intercept. The intercept, identified by *xx*, is “O1” for open-intercept one, or “C1” for close-intercept one.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1068E UNABLE TO OBTAIN STORAGE FOR *xx* INTERCEPT, RC=*rrrrrrrr*

Explanation

During Record level monitoring initialization, an error specified as *rrrrrrrr* was encountered during an attempt to obtain common storage for a product control block. The intercept, identified by *xx*, is “O1” for open-intercept one, or “C1” for close-intercept one.

User response

Investigate a potential shortage of common storage and restart the product. If the problem continues, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1069E UNABLE TO LOCATE IDA0200T

Explanation

During Record level monitoring initialization, a required operating system module could not be located.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1070I TCP/IP STREAMING DISABLED DUE TO USER SETTING

Explanation

This message indicates that the STAP_STREAM_EVENTS parameter is set to a value of `N`.

System action

The agent address space will not send data to the server. This feature is also referred to as Simulation Mode. The agent address space will perform all processing necessary to collect data consistent with the active policy.

User response

No action is required. To instruct the agent to stream data to the server, change the STAP_STREAM_EVENTS parameter value to *Y*.
Parent topic: Error message code descriptions

AUV1073W MAXIMUM ACTIVE SUBSYSTEMS EXCEEDED (1)

Explanation

The current iteration of the product being started would exceed the limit of one concurrently active subsystems on a single z/OS® system. Startup for the current iteration is terminated.

User response

If the current iteration of the product is needed, shut down one of the already active subsystems and then restart the current iteration. To display all currently active subsystems use the "`display,subsystems,all`" command.

Parent topic: Error message code descriptions

AUV1074E DUPLICATE SUBSYSTEM FOUND FOR SSID=*ssss*

Explanation

During product initialization, a duplicate product control block was encountered for the subsystem ID *ssss*.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1077I PII DATA NOT BEING TRANSMITTED DUE TO USER SETTING

Explanation

This message indicates that the FORCE_LOG_LIMITED parameter is set to a value of `Y`.

System action

When FORCE_LOG_LIMITED is set to `Y`, the S-TAP agent address space does not collect or send Personally Identifiable Identification (PII) data to the Guardium server. Record Level Monitoring (RLM) and CICS data is considered PII; therefore, it is not collected when FORCE_LOG_LIMITED is set to `Y`.

User response

No action is required. To collect and stream PII data, change the FORCE_LOG_LIMITED parameter value to `N`.
Parent topic: Error message code descriptions

AUV1080E ERROR IN NAME/TOKEN DELETE PROCESSING, RC=*rrrrrrrr*

Explanation

During product initialization, an error occurred that required product termination. During termination, an attempt was made to delete the product's NAME/TOKEN, but the NAME/TOKEN DELETE service encountered an error. *rrrrrrrr* contains the value returned in register 15.

System action

Product termination continues.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1081E GETMAIN FAILED FOR JSPB VECTOR TABLE, RC=*rrrrrrrr*

Explanation

During product initialization, the specified error *rrrrrrrr* occurred while attempting to obtain common storage for a product control block.

User response

Investigate a potential shortage of above-the-line common storage and restart the product. If the problem continues, contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1082W IEFU86 EXIT IS NOT DEFINED

Explanation

The Security Guardium® S-TAP® for Data Sets address space issues this message if it detects an inadequacy in the SMF exit definitions in z/OS V2.3 and later environments. During initialization, Security Guardium S-TAP for Data Sets verifies that the required SMF exit IEFU86 is defined to the system.

For z/OS V2.3 and later, IEFU86 must be defined in the SMFPRMxx system, at the system level of the PARMLIB member, or at the various subsystem levels for Security Guardium S-TAP for Data Sets to collect data set level auditing events.

User response

To audit data set level events, configure z/OS SMF to define the require SMF exits for the appropriate z/OS level. For more information, refer to Configuring the SMFPRMxx parameter library member.
Parent topic: Error message code descriptions

AUV1100E ACRONYM CHECK FAILED FOR GSSB

Explanation

An internal error occurred within the product during product initialization.

User response

Contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1101E INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING

Explanation

Main task startup was unable to obtain enough above-the-line private storage to initialize.

User response

Increase the amount of above-the-line private storage. If the problem persists, contact IBM® Support.

Parent topic: Error message code descriptions

AUV1102E ERROR OCCURRED IN CROSS-MEMORY INITIALIZATION

Explanation

An internal error occurred during main task startup.

User response

Contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1103E ATTACH FOR AUVPING FAILED, RC=*rrrrrrrr -ssss*

Explanation

During initialization of the Security Guardium® S-TAP® for Data Sets started task, an error was encountered during the attach of the subtask named AUVPING for the subsystem *SSSS*. The return code encountered is specified by *RRRRRRRR*.

User response

Ensure that the STEPLIB for the started task contains all of the load modules included with Security Guardium S-TAP for Data Sets. If the STEPLIB appears to correctly contain all of the product load modules, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1105E ATTACH FOR AUVSSRP FAILED, RC=*rrrrrrrr -ssss*

Explanation

During initialization of the Security Guardium® S-TAP® for Data Sets started task, an error was encountered during the attach of the subtask named AUVSSRP for the subsystem *SSSS*. The return code encountered is specified by *RRRRRRRR*.

User response

Ensure that the STEPLIB for the started task contains all of the load modules Included with Security Guardium S-TAP for Data Sets. If the STEPLIB appears to correctly contain all of the product load modules, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1105I SUBSYSTEM IS ACTIVE AND ENABLED

Explanation

This message indicates that the main product task has successfully started and is now active.

User response

No action is required.

Parent topic: Error message code descriptions

AUV1106I SUBSYSTEM INITIALIZATION IS COMPLETE

Explanation

This message is issued when the main product task has successfully completed initialization processing.

User response

No action is required.

Parent topic: Error message code descriptions

AUV1107I PRODUCT TERMINATION HAS BEEN REQUESTED

Explanation

This message is issued when the main product task has initiated subsystem shutdown processing, either due to a command request or because of an unrecoverable error condition.

User response

No action is required if this is due to a command request. If this is due to an unrecoverable error, restart the subsystem address space. Contact IBM® Software Support if the problems persist.

Parent topic: Error message code descriptions

AUV1111E UNABLE TO OBTAIN STORAGE FOR COMMON AREA ROUTINE, RC=*rrrrrrrr*

Explanation

Product subsystem initialization was unable to obtain a sufficient amount of storage to load a required module.

User response

Check and increase the amount available above- and below-the-line storage and restart the product. If the error persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1112E BLDL FAILED FOR *mmmmmmmm*, RC=*rrrrrrrr*

Explanation

During product subsystem initialization, a required load module was unable to be successfully located. The value *mmmmmmmm* identifies the load module and the value *rrrrrrr* specifies the internal return code in error.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task or in the system LINKLIST concatenation and then restart the product.
Parent topic: Error message code descriptions

AUV1113E UNABLE TO DETERMINE ORIGIN OF *mmmmmmmm*

Explanation

An error was encountered during product subsystem initialization while processing the product load module *mmmmmmmm*.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task or in the system LINKLIST concatenation and then restart the product
Parent topic: Error message code descriptions

AUV1115E INITIAL LOAD FAILED FOR *mmmmmmmm*

Explanation

During product subsystem initialization, a required load module (*mmmmmmmm*) did not load successfully.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task or in the system LINKLIST concatenation and then restart the product. In addition, check the available amount of above-the-line private storage available for the product started task. After correcting the problem restart the product. If the error cannot be determined, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1116E DIRECTED LOAD FAILED FOR *mmmmmmmm*

Explanation

During product subsystem initialization, a required load module (*mmmmmmmm*) did not load successfully.

User response

Verify that the load modules for the product are accessible either in a STEPLIB in the product started task or in the system LINKLIST concatenation and then restart the product.
Parent topic: Error message code descriptions

AUV1117E NON-ZERO RETURN CODE FROM SYSEVENT, RC=*rrrrrrrr -ssss*

Explanation

During product subsystem initialization, an error (*rrrrrrrr*) was encountered when attempting to make the product started task address space non-swappable for subsystem *ssss*.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1122E INVALID COMMAND SPECIFIED - *cccccccc -ssss*

Explanation

The product subsystem command parser received an error while processing the command (*cccccccc*) issued to the started task for subsystem ID *ssss*.

User response

Correct and re-issue the command.
Parent topic: Error message code descriptions

AUV1123E INVALID COMMAND SPECIFIED - *cccccccc -ssss*

Explanation

An invalid or null product subsystem command (*cccccccc*) was issued to the started task for subsystem ID *ssss*.

User response

Correct and re-issue the command.
Parent topic: Error message code descriptions

AUV1123W ACTIVE SUBSYSTEM DETECTED; PRODUCT-LEVEL MODULE NOT RE-INITIALIZED

Explanation

While a version of the product subsystem was active, an attempt was made to initiate the same product subsystem. The subsequent attempt to start the subsystem fails. Only one instance of the subsystem is allowed on a z/OS® image at a time.

User response

No action required. If you are attempting to initiate a new version of the subsystem, first shut down the currently executing version of the subsystem.
Parent topic: Error message code descriptions

AUV1124E EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*

Explanation

More operands than are allowed were specified for the DISPLAY command issued (*cccccccc*) to the product started task for subsystem ID *ssss*.

User response

Re-issue the command using the correct number of operands.
Parent topic: Error message code descriptions

AUV1125E INSUFFICIENT OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*

Explanation

The command entered contains fewer operands than the minimum required. The command entered is *cccccccc*. The subsystem ID is *ssss*.

User response

Re-issue the command using the correct number of operands.
Parent topic: Error message code descriptions

AUV1126E INVALID OPERAND SPECIFIED FOR COMMAND - *cccccccc -ssss*

Explanation

The command entered contains an invalid operand. The command entered is *cccccccc*. The subsystem ID is *ssss*.

User response

Correct the invalid operand and re-issue the command.
Parent topic: Error message code descriptions

AUV1127I SUBSYSTEM IS ACTIVE | INACTIVE AND ENABLED | DISABLED -*ssss*

Explanation

This message is issued in response to the DISPLAY SUBSYSTEM or DISPLAY ALL operator command and shows the ACTIVE or INACTIVE status of the product subsystem and whether or not the subsystem is ENABLED or DISABLED for the subsystem *ssss*.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1128E INVALID COMMAND SPECIFIED - *command*

Explanation

An unrecognized Security Guardium® S-TAP® for Data Sets operator command was issued to the started task where command is the unrecognized command.

User response

Issue a valid operator command to the started task.
Parent topic: Error message code descriptions

AUV1129I THERE ARE CURRENTLY NO SUBSYSTEMS -*ssss*

Explanation

This message is issued in response to the product operator command DISPLAY SUBSYSTEM ALL when no subsystems are located.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1130I SUBSYSTEM xxxx IS ACTIVE | INACTIVE AND ENABLED | DISABLED -*ssss*

Explanation

This message is issued in response to the DISPLAY SUBSYSTEM ALL operator command issued to subsystem *ssss* and shows the ACTIVE or INACTIVE status of each product subsystem as identified by *xxxx* and whether or not the subsystem is ENABLED or DISABLED.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1131I RULEDEFS ACTIVATED ON *mm/dd/yyyy* AT *hh:mm:ss* FROM MEMBER *mmmmmmmm -ssss*

Explanation

This message is issued in response to the DISPLAY RULEDEFS operator command to subsystem ID *ssss* and shows the date *mm/dd/yyyy* and time *hh:mm:ss* at which the active set of RULEDEFS was last activated as well as the member name (*mmmmmmmm*) from which they were activated.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1132I RULEDEFS NOT ACTIVATED -*ssss*

Explanation

This message is issued in response to the DISPLAY RULEDEFS operator command to subsystem ID *ssss* when no RULEDEFS were found to have been activated.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1136I PRODUCT-LEVEL TRACING IS ENABLED | DISABLED -*ssss*

Explanation

This message is issued in response to the DISPLAY TRACING operator command to subsystem ID *ssss* and shows whether or not the product tracing facility is ENABLED or DISABLED.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1137I SUBSYSTEM-LEVEL TRACING IS ENABLED | DISABLED -*ssss*

Explanation

This message is issued in response to the DISPLAY TRACING operator command to subsystem ID *ssss* and shows whether or not the subsystem tracing facility is ENABLED or DISABLED.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1138E EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*

Explanation

More operands than are allowed were specified for the ENABLE command issued (*cccccccc*) to the product started task for subsystem ID *ssss*.

User response

Re-issue the command using the correct number of operands.
Parent topic: Error message code descriptions

AUV1140I SMF MONITORING SUCCESSFULLY ENABLED – *SSSS*

Explanation

The ENABLE SMFM command was processed for the specified subsystem *SSSS*. The required SMF monitoring exits have been loaded and enabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1141I SUBSYSTEM IS NOW ENABLED -*ssss*

Explanation

This message is issued in response to the ENABLE SUBSYSTEM operator command and indicates that the subsystem *ssss* was successfully enabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1142I TCP/IP STREAM SUCCESSFULLY ENABLED -*ssss*

Explanation

This message is issued in response to the ENABLE INTERCEPTS operator command for subsystem *ssss* were successfully enabled.

System action

The agent address space will send data to the server in a manner that is consistent with the active policy.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1143I SMF MONITORING SUCCESSFULLY DISABLED –*SSSS*

Explanation

The DISABLE SMFM command was processed for the specified subsystem *SSSS*. The required SMF monitoring exits have been disabled and unloaded.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1144I TRACING FOR PRODUCT IS NOW ENABLED -*ssss*

Explanation

This message is issued in response to the ENABLE TRACING or ENABLE TRACING ALL operator command for subsystem ID *ssss* and indicates that product level tracing is now enabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1145I TRACING FOR SUBSYSTEM IS NOW ENABLED -*ssss*

Explanation

This message is issued in response to the ENABLE TRACING ALL operator command for subsystem ID *ssss* and indicates that subsystem level tracing is now enabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1146E EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*

Explanation

More operands than are allowed were specified for the DISABLE command issued (*cccccccc*) to the product started task for subsystem ID *ssss*.

User response

Re-issue the command using the correct number of operands.
Parent topic: Error message code descriptions

AUV1147I TCP/IP STREAM IS *EEEEEEEE -ssss*

Explanation

This message is issued in response to the operator command DISPLAY STREAM for subsystem *ssss*. The value *EEEEEEEE* indicates ENABLED or DISABLED.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1149I SUBSYSTEM IS NOW DISABLED -*ssss*

Explanation

This message is issued in response to the DISABLE SUBSYSTEM operator command and indicates that the subsystem *ssss* was successfully disabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1150I TCP/IP STREAM SUCCESSFULLY DISABLED -*ssss*

Explanation

This message is issued in response to the DISABLE STREAM operator command for subsystem *ssss*.

System action

The agent address space will not send data to the server. It will perform the steps that are necessary for data collection to be performed in a manner that is consistent with the active policy.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1151E SMF MONITORING DISABLE NOT SUCCESSFUL –*SSSS*

Explanation

The DISABLE SMFM command could not be processed for the specified subsystem *SSSS*. The SMF monitoring exits are still loaded and enabled.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1152I TRACING FOR PRODUCT IS NOW DISABLED -*ssss*

Explanation

This message is issued in response to the DISABLE TRACING or DISABLE TRACING ALL operator command for subsystem ID *ssss* and indicates that product level tracing is now disabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1153I TRACING FOR SUBSYSTEM IS NOW DISABLED -*ssss*

Explanation

This message is issued in response to the DISABLE TRACING ALL operator command for subsystem ID *ssss* and indicates that subsystem level tracing is now disabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1154E EXCESSIVE OPERANDS SPECIFIED FOR COMMAND - *cccccccc -ssss*

Explanation

More operands than are allowed were specified for the ACTIVATE command issued (*cccccccc*) to the product started task for subsystem ID *ssss*.

User response

Re-issue the command using the correct number of operands.
Parent topic: Error message code descriptions

AUV1155E SMF MONITORING ENABLE FAILED –*SSSS*

Explanation

The ENABLE SMFM command failed to process for the specified *SSSS*. The SMF monitoring exits are not loaded or enabled.

User response

Ensure that the STEPLIB for the started task contains all of the load modules required for the product. If no error can be found, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1156E SMF MONITORING ALREADY ENABLED –*SSSS*

Explanation

The ENABLE SMFM command was issued for the specified subsystem *SSSS* but the SMFEXIT1 exits are already enabled. The SMF exits are still loaded and enabled.

User response

No response is required.
Parent topic: Error message code descriptions

AUV1157E OPERANDS SPECIFIED FOR COMMAND - *command*

Explanation

An operator command as identified by command was issued to the started task for subsystem *SSSS*, but more operands were specified than are permitted for the particular command.

User response

Correct and reissue the operator command.
Parent topic: Error message code descriptions

AUV1158E SMF MONITORING ALREADY DISABLED –*SSSS*

Explanation

The DISABLE SMFM command was issued for the specified subsystem *SSSS* but the SMF monitoring exits are already disabled.

User response

No response is required.
Parent topic: Error message code descriptions

AUV1175I *DDDDDDDD* MEMBER ACTIVATION SUCCESSFUL –*SSSS*

Explanation

A policy member as identified by DDDDDDDD for subsystem SSSS was successfully activated.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1176E *DDDDDDDD* MEMBER ACTIVATION FAILED – SEE JESYSMSG FOR DETAILS –*SSSS*

Explanation

A policy member as identified by *DDDDDDDD* for subsystem *SSSS* could not be successfully activated. The JESYSMSG output data set for the started task contains details of the error(s) encountered.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1176I *dddddddd* MEMBER *mmmmmmmm* ACTIVATION FAILED - SEE JESYSMSG FOR DETAILS -*ssss*

Explanation

This message is issued in response to the ACTIVATE RULEDEFS operator command or the initial RULEDEFS activation (as indicated from the OPTIONS member for subsystem ID *ssss*) to show that the activation of the RULEDEFS from member *mmmmmmmm* was not successful due to syntax errors.

User response

Review the error messages in the JES SYSMSG output for the product started task, and then correct the errors and re-activate the RULEDEFS.
Parent topic: Error message code descriptions

AUV1177I *dddddddd* MEMBER *mmmmmmmm* ACTIVATION FAILED - FAILURE CODE *cccc -ssss*

Explanation

This message is issued in response to the ACTIVATE RULEDEFS operator command, or the initial RULEDEFS activation (as indicated from the OPTIONS member for subsystem ID *ssss)* to show that the activation of the RULEDEFS from member *mmmmmmmm* was not successful due to an internal error as denoted by *cccc*.

User response

Review any error messages in the JES SYSMSG output or the console log for the product started task to determine the possible cause of the error, then correct the errors and re-activate the RULEDEFS. If the problem persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1179E *DDDDDDDD* MEMBER ACTIVATION FAILED - FAILURE CODE *CCCCCCCC –SSSS*

Explanation

A policy member as identified by *DDDDDDDD* for subsystem *SSSS* could not be successfully activated. The failure code is identified by *CCCCCCCC*.

User response

Contact IBM® Technical Support.
Parent topic: Error message code descriptions

AUV1184E COMMAND VERB NOT UNIQUE - cccccccc -ssss

Explanation

More than one command exists that matches the abbreviation specified (*cccccccc*) for the command verb. The product subsystem processing the command was *ssss*.

User response

Re-issue the command, using a command verb abbreviation that more uniquely specifies the intended command.
Parent topic: Error message code descriptions

AUV1185E INVALID COMMAND SYNTAX SPECIFIED - *ssss*

Explanation

The command entered contains invalid syntax. The product subsystem processing the command was ssss.

User response

Review the command entered and correct the syntax.
Parent topic: Error message code descriptions

AUV1191E INVALID MODULE NAME SPECIFIED - *cccccccc*

Explanation

The command entered specifies an invalid module name. The command entered is *cccccccc*.

User response

Re-issue the command with a correct module name.
Parent topic: Error message code descriptions

AUV1192I MODULE *mmmmmmmm vvvv ffffffff dddddddd ttttt*

Explanation

Module header information is displayed, where *mmmmmmmm* is the name of the module, *vvvv* is the version, *ffffffff* is the FMID *dddddddd* is the assembly date and *ttttt* is the assembly time.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1193I MODULE *mmmmmmmm* LOCATED AT *aaaaaaaa* (*stgloc*)

Explanation

The module address (with offset if specified) is displayed, where *mmmmmmmm* is the name of the module, *aaaaaaaa* is the virtual storage address, and *stgloc* is the storage location ("PRIVATE" or "COMMON").

User response

No action is required.
Parent topic: Error message code descriptions

AUV1195E ERROR OCCURRED DURING FREEMAIN FOR GPB, RC=*rrrrrrrr*

Explanation

During initialization, the product encountered an error and determined that termination was necessary. As part of termination, an attempt was made to freemain the product control block, but the FREEMAIN service encountered an error. *rrrrrrrr* contains the value returned in register 15. Product termination continues.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1196E UNEXPECTED VCON COUNT FOR *xx* INTERCEPT; EXPECTED=*eee*, FOUND=*fff*

Explanation

While setting product intercept *xx*, An unexpected VCON count was encountered for a particular csect. The expected VCON count is *eee* and the actual VCON count is *fff*. This does not necessarily indicate a problem, but a problem is possible.

System action

An SVC memory dump is taken. Depending upon the particular intercept, product initialization might continue or terminate.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1200E UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA

Explanation

A service task of the main product started task was unable to obtain the required amount of above-the-line storage.

User response

Increase the amount of above-the-line storage for the product task. If the problem persists, contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1202E UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA

Explanation

A service task of the main product started task was unable to obtain the required amount of above-the-line storage.

User response

Increase the amount of above-the-line storage for the product task. If the problem persists, contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1203E UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA

Explanation

A product module was unable to obtain the required amount of above-the-line virtual storage.

User response

Increase the amount of above-the-line storage for the Security Guardium® S-TAP® for Data Sets started task and restart. If the problem persists, contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1204E UNABLE TO OBTAIN VIRTUAL STORAGE FOR WORKAREA

Explanation

A service task of the main product started task was unable to obtain the required amount of above-the-line storage.

User response

Increase the amount of above-the-line storage for the Security Guardium® S-TAP® for Data Sets started task. If the problem persists, contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1213E ERROR RETRIEVING SSRE

Explanation

An internal error was encountered.

User response

Contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1214E UNEXPECTED SSRE QUEUE ERROR

Explanation

An internal error was encountered.

User response

Contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1215E UNEXPECTED SSRE QUEUE ERROR

Explanation

An internal error was encountered.

User response

Contact IBM® Software Support.

Parent topic: Error message code descriptions

AUV1400I RECORD LEVEL MONITORING IS *EEEEEEEE -SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command DISPLAY RLM for subsystem *SSSS*. The value *EEEEEEEE* indicates *ENABLED* or *DISABLED*.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1401I RECORD LEVEL MONITORING INTERCEPTS ARE *EEEEEEEE* -*SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command DISPLAY RLM for subsystem *SSSS*. The value *EEEEEEEE* indicates ENABLED or DISABLED.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1402I CURRENT POLICY *EEE* -*SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command DISPLAY RLM for subsystem *SSSS*. The value *EEE* indicates either CONTAINS RLM FILTERS or DOES NOT CONTAIN RLM FILTERS.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1405I RECORD LEVEL MONITORING SUCCESSFULLY ENABLED -*SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command ENABLE RLM for subsystem *SSSS*.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1406W RECORD LEVEL MONITORING SUCCESSFULLY ENABLED, BUT NO RLM FILTERS EXIST IN CURRENT POLICY -*SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command ENABLE RLM for subsystem *SSSS*. The enable action was successful, but no filters specifying record level monitoring processing exist in the currently activated policy.

System action

Record level monitoring will not be performed.

User response

To perform record level monitoring, add record level monitoring definitions to the policy and activate it.
Parent topic: Error message code descriptions

AUV1408W POLICY CONTAINING RECORD LEVEL MONITORING FILTERS ACTIVATED, BUT RLM IS CURRENTLY DISABLED -*SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command ENABLE RLM for subsystem SSSS. The policy activation containing record level monitoring filters was successful, but record level monitoring processing is currently disabled.

System action

Record level monitoring will not be performed.

User response

To perform record level monitoring, issue the ENABLE RLM command for subsystem *SSSS*.
Parent topic: Error message code descriptions

AUV1410I PROCESSING OPTION SET - SOCKET_CONNECT_TIMEOUT=*nnnnn*

Explanation

This message is issued during product initialization to display the value (nnnnn) specified for the SOCKET_CONNECT_TIMEOUT keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1411E INVALID VALUE SPECIFIED FOR OPTION - SOCKET_CONNECT_TIMEOUT=*nnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the SOCKET_CONNECT_TIMEOUT option. The value *nnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1412I PROCESSING OPTION SET - OUTAGE_SPILLAREA_SIZE=*nnnnnnn*

Explanation

This message is issued during product initialization to display the value (nnnnnnn) specified for the OUTAGE_SPILLAREA_SIZE keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1413E INVALID VALUE SPECIFIED FOR OPTION – OUTAGE_SPILLAREA_SIZE=*nnnnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the OUTAGE_SPILLAREA_SIZE option. The value *nnnnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1414I PROCESSING OPTION SET - INTERNAL_BUFFER_SIZE=*nnnnnnn*

Explanation

This message is issued during product initialization to display the value (*nnnnnnn*) specified for the INTERNAL_BUFFER_SIZE keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1415E INVALID VALUE SPECIFIED FOR OPTION INTERNAL_BUFFER_SIZE=*nnnnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the INTERNAL_BUFFER_SIZE option. The value *nnnnnn* indicates the invalid value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1416I PROCESSING OPTION SET - APPLIANCE_SERVER_FAILOVER=a*

Explanation

This message is issued during product initialization to display the value a* specified for the APPLIANCE_SERVER_FAILOVER keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1417E INVALID VALUE SPECIFIED FOR OPTION - *keyword*=a*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the keyword. The *keyword* value indicates APPLIANCE_SERVER_FAILOVER_*n*, or its alternate specification, APPLIANCE_SERVER_*n*, where *n* is 1, 2, 3, 4, or 5. The value *a** indicates the invalid value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1418I PROCESSING OPTION SET - IAM_SMF_RECORD_ID = *nnn*

Explanation

This message is issued during product initialization to display the value *nnn* that is specified for the IAM_SMF_RECORD_ID keyword in the OPTIONS member. This keyword identifies the SMF record ID for the IAM records.

User response

For Security Guardium® S-TAP® for Data Sets to report IAM access, specify the value *nnn* in the control data set IAM_SMF_RECORD_ID option.
Parent topic: Error message code descriptions

AUV1419E INVALID VALUE SPECIFIED FOR OPTION - IAM_SMF_RECORD_ID = *nnn*

Explanation

While processing the subsystem options in the OPTIONS member during product initialization, an incorrect value was encountered for the IAM_SMF_RECORD_ID option. The value *nnn* indicates the invalid value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1420I PROCESSING OPTION SET - ACF_SMF_RECORD_ID = *nnn*

Explanation

This message is issued during product initialization to display the value specified for the ACF_SMF_RECORD_ID keyword in the OPTIONS member. This keyword identifies the SMF record ID for the ACF2 records.

User response

For Security Guardium® S-TAP® for Data Sets to report access failures to a unique record ID, specify the value *nnn* in the control data set ACF_SMF_RECORD_ID option.
Parent topic: Error message code descriptions

AUV1421E INVALID VALUE SPECIFIED FOR OPTION - ACF_SMF_RECORD_ID = *nnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the ACF_SMF_RECORD_ID option. The value nnn indicates the invalid value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1422I PROCESSING OPTION SET - APPLIANCE_SERVER_LIST(*nnn*)

Explanation

This message is issued during product initialization to display the value specified for the APPLIANCE_SERVER_LIST keyword in the OPTIONS member. This value *nnn* identifies one of the following selected options:

FAILOVER
: One appliance connection is active at a time. If the connection to the primary appliance is lost, a failover action occurs, which results in an attempt to connect to the next available server. The appliance attempts to reconnect to the primary server at intervals of 12 times the PING_RATE.

MULTI_STREAM
: An appliance connection is established for each server that is listed by the APPLIANCE_SERVER_n or APPLIANCE_SERVER_FAILOVER_n parameter. When a connection is lost, Security Guardium® S-TAP® for Data Sets audit events continue to be spread over the remaining appliance connections. Any lost connections are retried at regular intervals of 12 times the PING_RATE.

HOT_FAILOVER
: Keeps each connected Guardium appliance active via pings. If the primary Guardium appliance becomes unavailable and failover occurs, *HOT_FAILOVER* maintains the activity of the primary appliance policy.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1423E INVALID VALUE SPECIFIED FOR OPTION - APPLIANCE_SERVER_LIST(*nnn*)

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the APPLIANCE_SERVER_LIST option. The value *nnn* indicates the incorrect value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1424I PROCESSING OPTION SET - MEGABUFFER_COUNT =*nnnnnnn*

Explanation

This message is issued during product initialization to display the value (*nnnnnnn*) that is specified for the MEGABUFFER_COUNT keyword in the OPTIONS member.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1425E INVALID VALUE SPECIFIED FOR OPTION MEGABUFFER_COUNT =*nnnnnnn*

Explanation

During product initialization, while processing the subsystem options in the OPTIONS member, an incorrect value was encountered for the MEGABUFFER_COUNT option. The value *nnnnnnn* indicates the incorrect value.

User response

Correct the specified option keyword and restart.
Parent topic: Error message code descriptions

AUV1438I SMF MONITORING IS *EEEEEEEE -SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command DISPLAY SMFEXIT1 for subsystem *SSSS*. The value *EEEEEEEE* indicates *ENABLED* or *DISABLED*.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1439I SMF MONITORING EXITS ARE *EEE -SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets operator command DISPLAY SMFM for subsystem *SSSS*. The value *EEE* indicates ACTIVE/LOADED or NOT ACTIVE/LOADLED.

User response

No action is required.
Parent topic: Error message code descriptions

AUV1450W SMF RECORDING TEST FAILED, RC=*cc*, TYPE=*nnnn*, SUBSYSTEM=*ssss*

Explanation

The Security Guardium® S-TAP® for Data Sets address space issues this message if it detects an inadequacy in the SMF environment. During initialization,Security Guardium S-TAP for Data Sets tests z/OS® MVS™ SMF to determine if SMF is collecting the record types that are necessary for data set level auditing. The S-TAP address space issues this message for each SMF record type *nnnn*, and z/OS MVS subsystem *ssss*, for which the test fails. RC *cc* identifies one of the following return codes:

16
: SMF is not active or has ended abnormally.

36
: Information for the specified record type is not being recorded.

User response

To audit data set level events, configure z/OS MVS SMF to collect the required SMF records. For more information, refer to Configuring the SMFPRMxx parameter library member.
Parent topic: Error message code descriptions

AUV1747E SUBSYSTEM IS NOT ACTIVE OR ENABLED

Explanation

This message is issued when, during the activation of a policy, the Security Guardium® S-TAP® for Data Sets subsystem is found to be disabled or inactive. The policy is not activated.

User response

Ensure that the Security Guardium S-TAP for Data Sets started task has been started and that the subsystem is enabled and the hooks are active. If the problem persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV1748W POLICY CONTAINING RECORD LEVEL MONITORING FILTERS ACTIVATED, BUT RLM IS CURRENTLY DISABLED -*SSSS*

Explanation

This message is issued in response to the Security Guardium® S-TAP® for Data Sets policy pushdown operation for subsystem *SSSS*. The policy pushdown containing record level monitoring filters was successful, but record level monitoring processing is currently disabled.

System action

Record level monitoring will not be performed.

User response

To perform record level monitoring, issue the ENABLE RLM command for subsystem *SSSS*.
Parent topic: Error message code descriptions

AUV2000E INSUFFICIENT VIRTUAL STORAGE FOR PRODUCT PROCESSING

Explanation

During an attempt to intercept an OPEN/CLOSE event, Security Guardium® S-TAP® for Data Sets was unable to obtain enough virtual storage to perform processing.

User response

Increase the amount of virtual storage for the job. If the error persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2030E UNRECOGNIZED INTERCEPT ID ENCOUNTERED (*XX*)

Explanation

Security Guardium® S-TAP® for Data Sets received control with unexpected intercept parameters.

User response

This is an unexpected internal condition. If product maintenance was recently applied, ensure that all steps in the HOLDDATA were performed. If they were, record the ID *XX* and contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2040E ERROR OCCURRED DURING SWAREQ PROCESSING FOR JCT, RC=*rrrrrrrr*

Explanation

During interception of an OPEN or CLOSE event, an internal error specified as *rrrrrrrr* occurred while attempting to access a system control block.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2041E ERROR OCCURRED DURING SWAREQ PROCESSING FOR SCT, RC=*rrrrrrrr*

Explanation

During interception of an OPEN or CLOSE event, an internal error specified as *rrrrrrrr* was encountered while attempting to access a system control block.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2042E ERROR OCCURRED DURING SWAREQ PROCESSING FOR JMR, RC=*rrrrrrrr*

Explanation

During interception of an OPEN or CLOSE event, an internal error specified as *rrrrrrrr* occurred while attempting to access a system control block.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2097I JCT UNAVAILABLE FOR JSPB LOOK-UP FOR ASID *xxxx*

Explanation

During interception of an OPEN or CLOSE event, Security Guardium® S-TAP® for Data Sets was unable to locate a product control block for the address space with the ASID *xxxx*.

System action

Processing is bypassed for the current job.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2098I ASID *xxxx* EXCEEDS GJVT MAX; ASVTMAXU=*xxxxxxxx*

Explanation

During interception of an OPEN or CLOSE event, Security Guardium® S-TAP® for Data Sets detected an unexpected error for the address space with the ASID *xxxx*. The system value for ASVTMAX *xxxxxxxx* is also displayed.

System action

Processing is bypassed for the current job.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2104E ERROR OCCURRED IN FREEMAIN OF AUVSMFX1, RC=*RRRRRRRR*

Explanation

During termination processing of the Security Guardium® S-TAP® for Data Sets started task or during the DISABLE of the SMFEXIT1 exits, the storage occupied by the module AUVSMFX1 could not be successfully freed. The error code encountered is specified by *RRRRRRRR*.

User response

No noticeable effect on system operations should be noticed as, although the module is located in Extended CSA, it consumes only a few kilobytes of storage. However, the cause of the error should be investigated by contacting IBM® Software Support.
Parent topic: Error message code descriptions

AUV2170I ATTEMPTING TO CONNECT TO THE GUARDIUM APPLIANCE

Explanation

This is an informational message issued during product initialization indicating initialization progress.

User response

None required.
Parent topic: Error message code descriptions

AUV2171I CALL TO GUARDIUM APPLIANCE SUCCESSFUL

Explanation

This is an informational message issued during product initialization indicating that the z/OS® host component of successfully connected to Guardium® system.

User response

No action is required.
Parent topic: Error message code descriptions

AUV2172E *function* CALL TO GUARDIUM APPLIANCE FAILED

Explanation

An attempt to communicate with the Guardium® system failed. Before reporting the failure, the agent retried the request the number of times specified on the APPLIANCE_RETRY_INTERVAL parameter for the number of iterations specified on the APPLIANCE_CONNECT_RETRY_COUNT parameter. The *function* will be one of the following:

INIT
: Guardium system initialization, which occurs when the started task starts.

PING
: Cyclical pings to the system that report the agent's status.

SEND-SMF
: Agent transmission of the audit records to the Guardium system.

If any one of these service requests fail, the agent address space is terminated.

User response

Correct any communications issue causing this failure and restart the agent started task. Contact IBM® Software Support for further assistance.
Parent topic: Error message code descriptions

AUV2173E *function* CALL TO GUARDIUM APPLIANCE FAILED, RC = *rc* RC_STP= *rc* RS_STP= *rs* RC_GDM= *rc* RC_PB = *rc* RC_LST= *rc* RS_LST= *rs*

Explanation

An attempt to communicate with the Guardium® system failed. Before reporting the failure, the agent retried the request the number of times specified on the APPLIANCE_RETRY_INTERVAL parameter for the number of iterations specified on the APPLIANCE_CONNECT_RETRY_COUNT parameter. The function will be one of the following:

INIT
: Guardium system initialization, which occurs at started task initialization.

PING
: Cyclical pings to the system that reports the agent's status.

SEND-SMF
: Agent transmission of the audit records to the Guardium system. If any one of these service requests fail, the agent address space is terminated.

The *rc* and *rs* text is replaced with numeric values that can assist IBM® Support with problem diagnosis, if the problem persists.

User response

Correct any communications issue causing this failure and restart the agent started task. Contact IBM Support for further assistance.
Parent topic: Error message code descriptions

AUV2174E SPILL FILE FULL, DATA LOSS MIGHT OCCUR

Explanation

Connection to the Guardium® system has unexpectedly terminated and the spill file with SPILL_BUFFER size is now full. Data loss can occur if this condition continues.

User response

Ensure that the Guardium system is communicating. Increase the SPILL_BUFFER value to increase the amount of data that can be written to the spill file.
Parent topic: Error message code descriptions

AUV2175E CONNECTION LOST WITH NO SPILL FILE, DATA LOSS MIGHT OCCUR

Explanation

The connection to the Guardium® system has unexpectedly terminated. SPILL_BUFFER was not specified in the configuration member.

User response

Determine the cause of the network interruption and correct the problem so that the connection can be re-established. To minimize data loss, specify a SPILL_BUFFER.
Parent topic: Error message code descriptions

AUV2176E UNABLE TO OBTAIN STORAGE, DATA LOSS MIGHT OCCUR

Explanation

An attempt to allocate storage for additional data failed.

User response

Ensure that a sufficient region size is provided in the started task JCL.
Parent topic: Error message code descriptions

AUV2177E RULEDEF NOT ACTIVATED - CHECK SYSPRINT FOR REASON

Explanation

An attempt to process a policy pushdown failed. No RULEDEF was activated as a result.

User response

Check the SYSPRINT for the detailed reason on what caused the failure. Correct the issue, and reissue a policy pushdown.
Parent topic: Error message code descriptions

AUV2178I SPILL FILE IS *xx*% FULL

Explanation

This message is issued while the spill file is in use. It indicates that the spill file has been filled to the percentage indicated.

User response

No action is required.
Parent topic: Error message code descriptions

AUV2179E UNABLE TO OBTAIN REQUESTED STORAGE FOR INTERNAL_BUFFER_SIZE: dddd. PROCESSING CONTINUES.

Explanation

An attempt to allocate storage for the internal buffer has failed. The started task remains up, but data processing does not run as efficiently.

User response

Ensure that a sufficient region size is provided in the started task JCL, or decrease the amount specified for INTERNAL_BUFFER_SIZE in the OPTIONS member. If the problem persists, contact IBM Software Support.
Parent topic: Error message code descriptions

AUV2180W WRITING TO SPILL FILE

Explanation

The connection to the Guardium system has been lost. All data is now being written to a spill file. The data in the spill file will be written to the Guardium system when the connection is restored.

User response

Determine the cause of the network interruption and correct the problem so that the connection can be re-established.
Parent topic: Error message code descriptions

AUV2181I NO LONGER WRITING TO SPILL FILE

Explanation

The connection to the Guardium system has been restored, and the agent is no longer writing to the spill file.

User response

No action is required.
Parent topic: Error message code descriptions

AUV2182I CONNECTION ESTABLISHED TO *x*

Explanation

An attempt to connect to the Guardium system was successful, where *x* is the system with which a connection has been made.

User response

No action is required.
Parent topic: Error message code descriptions

AUV2183W STORAGE SHORTAGE DETECTED; ONE OR MORE EVENTS NOT RECORDED

Explanation

An attempt to allocate virtual storage for an internal product control block failed. Without the control block, the data for the event cannot be captured.

User response

Ensure that a sufficient region size is provided in the started task JCL. A region size of at least 96M is recommended when a large number of events are being monitored.

If the problem persists, evaluate the amount of data that is being captured as defined by the policy. Monitoring a very large number of events can cause storage shortages, especially when Record Level Monitoring (RLM) is being used.

Parent topic: Error message code descriptions

AUV2184W STORAGE SHORTAGE RELIEVED; EVENT RECORDING RESUMED. EVENTS LOST=????????

Explanation

A previous virtual storage shortage was resolved, allowing event recording to be resumed. EVENTS LOST=*????????* indicates the number of events that could not be recorded.

User response

No action is required.
Parent topic: Error message code descriptions

AUV2185I UNEXPECTED PRODUCT STATE DETECTED. ATTEMPTING RESTART.

Explanation

Indicators in product control blocks conflict with the current product state. This could be caused by a non-standard product shutdown or an unexpected product termination. The product will attempt to correct the environment and continue to re-initialize.

User response

No action is required.
Parent topic: Error message code descriptions

AUV2186E UNABLE TO RESOLVE HOST NAME *a**

Explanation

During product initialization, one of the host names (*a**) specified for the APPLIANCE_SERVER or APPLIANCE_SERVER_n option could not be resolved to a valid IP address.

User response

Ensure that all the host names specified in the OPTIONS member are correct and can be resolved to IP addresses. Correct the configuration if needed and restart.
Parent topic: Error message code descriptions

AUV2900E INVALID STORAGE REQUEST FOR CONTROL BLOCK *nnnn -ssss*

Explanation

An internal error occurred while attempting to obtain a control block identified by *nnnn* subsystem ID *ssss*.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2901E INSUFFICIENT VIRTUAL STORAGE FOR CONTROL BLOCK *nnnn -ssss*

Explanation

Sufficient storage was not available to obtain a required control block identified by *nnnn* subsystem ID *ssss*.

User response

Attempt to increase above-the-line or below-the-line storage for the job receiving the error message. If the error persists, contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2902E ACRONYM CHECK FAILED WHILE ATTEMPTING TO FREE *nnnn*, DATA=*dddd -ssss*

Explanation

An internal error occurred while attempting to free a control block identified by *nnnn* with the invalid data identified by *dddd* for subsystem ID *ssss*.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV2903E FAILURE OCCURRED DURING FREEMAIN FOR *nnnn -ssss*

Explanation

An internal error occurred while attempting to free a control block identified by *nnnn* subsystem ID *ssss*.

User response

Contact IBM® Software Support.
Parent topic: Error message code descriptions

AUV3000E ERROR ENABLING AUVFROUT: EIBRCODE=*NNNNNNNNNNN*

Explanation

While running the Program List Table Program Initialization module AUVPLTPI, an error was encountered attempting to enable the XFCFROUT Global User Exit program AUVFROUT. The value *NNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response

Interpret the error codes using the documentation provided in the CICS Transaction Server System Programming Reference manual, “Appendix B. EXEC interface block (EIB) response and function codes." Contact IBM Software Support if you are unable to determine the cause of the problem.
Parent topic: Error message code descriptions

AUV3001E ERROR OBTAINING GWA ADDR: EIBRCODE=*NNNNNNNNNNN*

Explanation

While running the Program List Table Program Initialization module AUVPLTPI, an error was encountered regarding an attempt to obtain the address of the Global Work area. The value *NNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response

Interpret the error codes using the documentation provided in the CICS Transaction Server System Programming Reference manual, “Appendix B. EXEC interface block (EIB) response and function codes." Contact IBM Software Support if you are unable to determine the cause of the problem.
Parent topic: Error message code descriptions

AUV3003E ERROR STARTING AUVFROUT: EIBRCODE=*NNNNNNNNNNN*

Explanation

While running the Program List Table Program Initialization module AUVPLTPI, an error was encountered regarding an attempt to start the XFCFROUT Global User Exit AUVFROUT. The value *NNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response

Interpret the error codes using the documentation provided in the CICS Transaction Server System Programming Reference manual, “Appendix B. EXEC interface block (EIB) response and function codes." Contact IBM Software Support if you are unable to determine the cause of the problem.
Parent topic: Error message code descriptions

AUV3004I AUVPLTPI XFCFROUT GLOBAL USER EXIT SUCCESSFULLY ENABLED AND STARTED

Explanation

While running the Program List Table Program Initialization module AUVPLTPI, the XFCFROUT Global User Exit AUVFROUT was successfully enabled and started.

User response

No action is required.
Parent topic: Error message code descriptions

AUV3005E ERROR STOPPING AUVFROUT: EIBRCODE=*NNNNNNNNNNN*

Explanation

While running the Program List Table Program Termination module AUVPLTPS, an error was encountered regarding an attempt to stop the XFCFROUT Global User Exit AUVFROUT. The value *NNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response

Interpret the error codes using the documentation provided in the CICS Transaction Server System Programming Reference manual, “Appendix B. EXEC interface block (EIB) response and function codes." Contact IBM Software Support if you are unable to determine the cause of the problem.
Parent topic: Error message code descriptions

AUV3006E ERROR OBTAINING GWA ADDR: EIBRCODE=*NNNNNNNNNNN*

Explanation

While running the Program List Table Program Termination module AUVPLTPS, an error was encountered regarding an attempt to obtain the address of the Global Work area. The value *NNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response

Interpret the error codes using the documentation that is provided in the CICS Transaction Server System Programming Reference manual, Appendix B. EXEC interface block (EIB) response and function codes. Contact IBM Software Support if you are unable to determine the cause of the problem.
Parent topic: Error message code descriptions

AUV3008E ERROR DISABLING AUVFROUT: EIBRCODE=*NNNNNNNNNNN*

Explanation

While running the Program List Table Program Termination module AUVPLTPS, an error was encountered regarding an attempt to disable the XFCFROUT Global User Exit AUVFROUT. The value *NNNNNNNNNNN* represents the EXEC Interface Block error and response codes.

User response

Interpret the error codes using the documentation provided in the CICS Transaction Server System Programming Reference manual, “Appendix B. EXEC interface block (EIB) response and function codes." Contact IBM Software Support if you are unable to determine the cause of the problem.
Parent topic: Error message code descriptions

AUV3009I AUVPLTPS XFCFROUT GLOBAL USER EXIT SUCCESSFULLY STOPPED AND DISABLED

Explanation

While running the Program List Table Program Termination module AUVPLTPS, the XFCFROUT Global User Exit AUVFROUT was successfully stopped and disabled.

User response

No action is required.
Parent topic: Error message code descriptions

AUV3010W CICS PLTPI INSTALLED BUT CICS_SUPPORT NOT SPECIFIED IN OPTIONS

Explanation

The CICS Support Program List Table Program Initialization program AUVPLTPI was defined to CICS, but the CICS_SUPPORT parameter was not enabled in the OPTIONS start-up parameters for the Security Guardium® S-TAP® for Data Sets started task.

User response

To use full CICS support within the product, you must specify CICS_SUPPORT=ENABLE in the OPTIONS parameters defined to the started task. Make the necessary changes to the OPTIONS parameters and restart the product.
Parent topic: Error message code descriptions